GeoVision inc
The Vision of Security

GV-ASManager

Manuale utente V1.1

© 2008 GeoVision Inc. Tutti i diritti riservati.
In base alle leggi sul copyright, questo manuale non può essere copiato, né nella sua interezza, né parzialmente, senza il consenso scritto di GeoVision.

Sono stati fatti tutti gli sforzi possibili per far sì che le informazioni contenute nel presente manuale siano accurate. GeoVision non è responsabile di errori di stampa o di ufficio.

GeoVision, Inc.
9F, No. 246, Sec. 1, Neihu Rd.,
Neihu District, Taipei, Taiwan
Tel: +886-2-8797-8377
Fax: +886-2-8797-8335
http://www.geovision.com.tw

Marchi di fabbrica usati nel presente manuale: *GeoVision*, il logo *GeoVision* e i prodotti della serieGV sono marchi di fabbrica di GeoVision, Inc. *Windows* e *Windows XP* sono marchi di fabbrica di Microsoft Corporation.

Giugno 2008

Indice

Capitolo 1 Introduzione 3
1.1 Caratteristiche principali 4
1.2 Concetti 5

Capitolo 2 Installazione 7
2.1 Installazione di ASManager 7
2.2 Registrazione 8

Capitolo 3 La schermata principale di ASManager 9
3.1 Schermata principale 9
3.1.1 Barra degli strumenti 10
3.2 Stato dispositivo 11
3.2.1 Controllori nella finestra 12
3.3 Monitoraggio finestre 12
3.3.1 Comandi all'interno della finestra 13
3.3.2 Personalizzazione di una finestra di monitoraggio 14
3.3.3 Organizzare le finestre di monitoraggio 15

Capitolo 4 Impostazioni 17
4.1 Diagramma di flusso delle impostazioni 17
4.2 Aggiungere controllori 18
4.2.1 Fase 1: configurazione di un controllore per la porta 18
4.2.2 Fase 2: configurare una porta 19
4.3 Impostazione tessere 21
4.3.1 Aggiungere una singola scheda 22
4.3.2 Aggiungere un gruppo di tessere 24
4.3.3 Importare/Esportare dati di tessere 24
4.4 Impostazione delle Schedulazioni Settimanali 26
4.4.1 Fase 1: Impostazione fuso orario 26
4.4.2 Fase 2: Impostazione delle Schedulazioni Settimanali 28
4.4.3 Fase 3: Impostazione delle ferie 30
4.5 Impostazione gruppi di accesso 31
4.6 Impostazione dei titolari di tessera 32
4.6.1 Aggiungere un titolare di tessera 32
4.6.2 Assegnare una tessera ad un titolare 33
4.6.3 Invio allarmi SMS 34
4.6.4 Personalizzazione di un campo dati 34
4.6.5 Importazione/Esportazione dei dati del titolare di tessera 35

Capitolo 5 Integrazione video 37
5.1 Mappatura delle videocamere 37
5.2 Accesso a Vista live 39
5.3 Accedere all'immagine video 39
5.4 Finestra Multiview 40
5.4.1 Aggiunta di una visualizzazione a matrice 41
5.5 Recupero dei video registrati 42

Capitolo 6 ASLog 45

Capitolo 7 Altre funzioni 47
7.1 Impostazione utente di sistema 47
7.1.1 Aggiungere un nuovo utente 47
7.1.2 Modifica di un utente esistente 49
7.1.3 Modifica della password al momento del login 49
7.2 Impostazione notifica 50
7.2.1 Impostazione del server SMS 50
7.2.2 Impostazione del server e-mail 51
7.2.3 Impostazione della notifica 52
7.3 Configurazione di avvio e di backup 53

Capitolo 8 ASRemote 55
8.1 Installazione di ASRemote 55
8.2 La finestra di ASRemote 56
8.2.1 Barra degli strumenti 57
8.3 Connessione a ASManager 58

Capitolo 9 ASWeb 61
9.1 Connessione a ASManager 61
9.2 Accedere ai log 63
9.2.1 Impostazione dei criteri di ricerca 63
9.2.2 Icone della finestra di log 64
9.2.3 Esportare i log 65
9.2.4 Definizione delle colonne 65

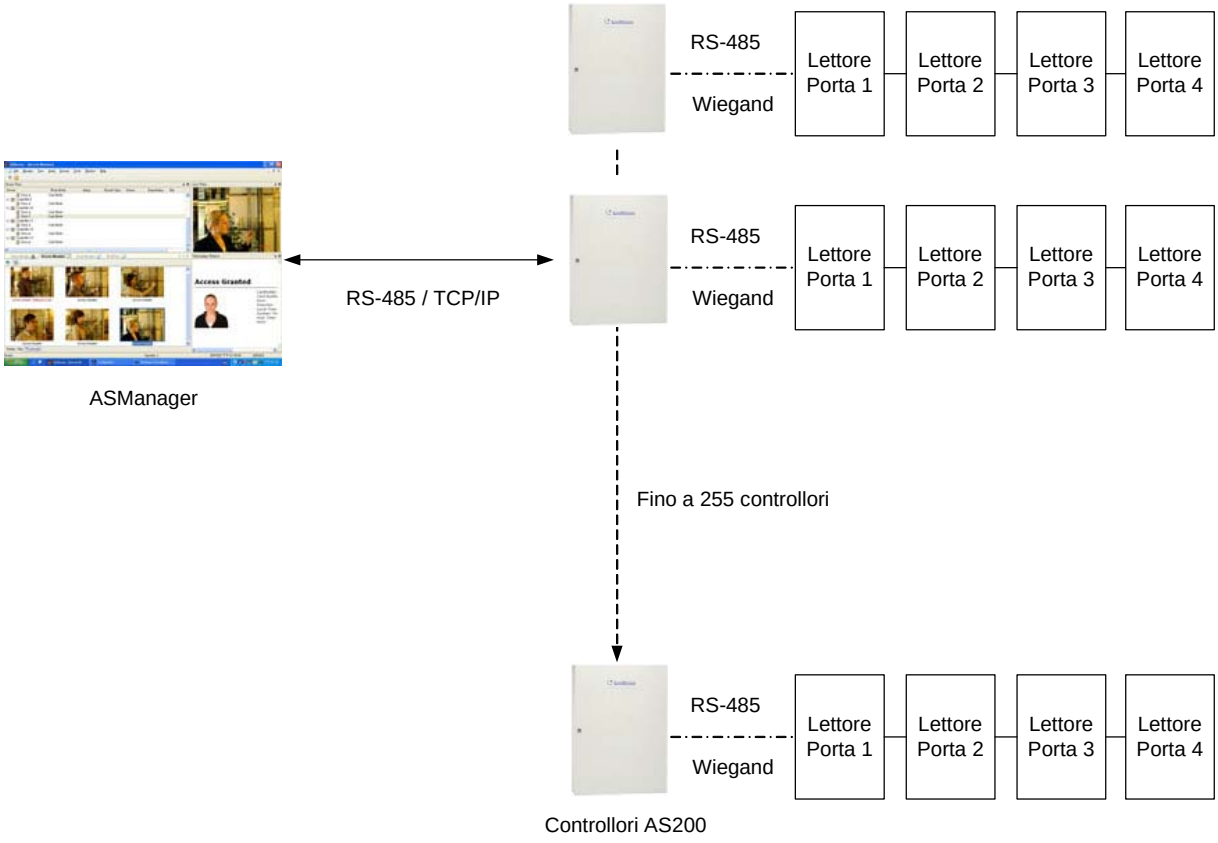
Capitolo 10 Risoluzione dei problemi 67

Appendice …… 73
A. Dispositivi IP compatibili 73
B. Notifiche degli eventi 74
C. Simboli degli allarmi e-mail e SMS 78

Capitolo 1 Introduzione

ASManager e il controllore AS200 sono la combinazione che permette di avere il controllo completo degli ingressi della vostra azienda. Un singolo ASManager può monitorare fino a 255 controllori AS200.

Il diagramma che segue è un esempio di come è possibile configurare ASManager e il controllore AS200.



1.1 Caratteristiche principali

ASManager

- Controlla fino a 255 controllori GV-AS
- Fino a 256 fusi orari e schedulazioni settimanali
- Fino a 10.000 tessere
- Fino a 1.000 utenti del sistema
- Piano ferie per 14 mesi
- Più tessere per utente
- Quattro (4) diverse modalità di accesso: Modo solo tessera (predefinita), modo Codice PIN e Tessera , modalità Tessera o Comune, modo Rilascio
- Tessere di registrazione in modalità batch
- Allarmi per porte: apertura tenuta porta, porta forzata, manomessa o accesso negato
- Operazione coercitiva
- Capacità anti-passback
- Porta a bussola doppia
- Importazione/esportazione della tessera e dati del titolare della tessera in formato file Access o Excel
- Matrici definite dall'utente di visualizzazione multipla a 16 canali
- Predisposizione schermata definita dall'utente e supporto doppio di visualizzazione del monitor
- Notifica SMS o e-mail con contenuto definito dall'utente, scatto video e foto del titolare della tessera
- Integrazione video con dispositivi IP GeoVision (GV-System, GV-NVR, GV-Video Server, GV-Compact DVR, GV-IP Camera) e con telecamere IP di terzi.

ASLog

- Le informazioni del log con il video e l'istantanea corrispondenti

ASRemote

- Monitoraggio illimitato ASManagers su Internet
- Monitoraggio remoto delle porte, riproduzione video, funzionamento porta

ASWeb

- Interfaccia web per ricerca dello storico del registro con video e istantanea corrispondenti
- Esportazione del registro in formato Excel, Testo, HTML.

1.2 Concetti

La comprensione dei seguenti concetti può aiutare nella lettura del manuale.

Schedulazione settimanale	La schedulazione settimanale consiste nell'indicazione di determinati giorni della settimana in cui l'utente può accedere a un sito sicuro. Per i dettagli, vedere *4.4 Impostazione della schedulazione settimanale.*
Gruppo di accesso	Un gruppo di accesso è costituito da una serie di titolari di tessere con restrizioni di accesso allo stesso luogo e negli stessi orari. Per i dettagli vedere *4.5 Creazione di un gruppo di accesso..*
Condizione di allarme	La condizione di allarme viene monitorata mediante dispositivi sensibili e può attivare gli allarmi. Il controllore AS200 può monitorare 3 sensori, come quello dello stato della porta, il rilevatore di fumo e quello di manomissioni. Il controllore AS200 fornisce anche 3 relè di uscita per l'attivazione e la disattivazione del blocco elettrico, della sirena e dello sblocco della porta di emergenza, se si verifica una condizione di allarme. Per le impostazioni delle condizioni di allarme *4.2.2 Fase 2: configurare una porta*. Per la configurazione degli ingressi e delle uscite vedere *Guida di installazione dell'hardware del controllore AS200*.
Anticoercizione	Se una persona è costretta sotto minaccia ad aprire la porta, può inserire il suo PIN più un altro numero per attivare l'allarme e inviare un segnale ad ASManager perché allerti la polizia. Ad esempio, se il PIN è 5555 e si inserisce 5556. La porta si apre normalmente (accesso garantito) e si attiva l'allarme. La funzione è abilitata nel sistema per impostazione predefinita.
Anti-passback	La funzione è studiata per prevenire la condivisione della tessera e imporre l'uso dei lettori in entrata e in uscita. Se una tessera viene usata sul lettore in entrata, prima di essere valida di nuovo per l'accesso deve essere usata su un lettore in uscita. Per le impostazioni vedere *4.2.2 Fase 2: configurare una porta*.
Sincronizzazione	La funzione è anche detta "porta a bussola" o "interlocking". Essa sincronizza due porte controllate, consentendo l'apertura solo di una alla volta. La funzione non permette di sbloccare una porta, se l'altra è aperta. Se entrambe le porte sono aperte contemporaneamente, l'allarme sarà attivo. Per le impostazioni vedere *4.2.1 Fase 1: configurare il controllore di una porta*.

Regola A/B delle due persone	La porta si sblocca solo quando due tessere assegnate vengono presentate insieme. Per le impostazioni vedere *4.3.1 Aggiungere una singola tessera*.
Dispositivo IP	Il dispositivo video è connesso a ASManager attraverso la rete. ASManager consente di accedere ai video live, non solo dai dispositivi IP GeoVision (GV-System, GV-NVR, GV-Video Server, GV-Compact DVR e GV-IP Camera) ma anche da alcune telecamere IP di terze parti. Per i dettagli vedere *Integrazione video* nel Capitolo 5.

Capitolo 2 Installazione

2.1 Installazione di ASManager

È necessario usare Keypro con il programma ASManager. Sono disponibili i seguenti Keypro:

- **Keypro 4** è usato per la connessione di un massimo di 4 controllori AS200.
- **Keypro 10** è usato per la connessione di un massimo di 10 controllori AS200.
- **Keypro 30** è usato per la connessione di un massimo di 30 controllori AS200.
- **Keypro 50** è usato per la connessione di un massimo di 50 controllori AS200.
- **Keypro 255** è usato per la connessione di un massimo di 255 controllori AS200.

Requisiti di sistema

Requisiti del disco rigido per il computer di installazione di ASManager: 2,4 G o superiore.

Per installare i driver Keypro:

Inserire il CD contenente il software nel computer e automaticamente apparirà una finestra pop-up. Selezionare **Install or Remove GeoVision GV-Series Driver (Installa o rimuovi il driver GeoVision serie GV)** e fare clic su **Install Geovision USB Devices Driver (Installa il driver dei dispositivi USB Geovision)**.

Per installare ASManager:

Inserire il CD contenente il software nel computer e automaticamente apparirà una finestra pop-up. Selezionare **Install GeoVision V1.1 Access Control System (Installa il sistema di controllo dell'accesso GeoVision V1.1)** fare clic su **GeoVision Access Control System (Sistema di controllo accessi GeoVision)** e seguire le istruzioni a video per completare l'installazione.

2.2 Registrazione

Per avviare ASManager, fare clic su **Start**, andare su **Programmi**, selezionare **AS200** e fare clic su **ASManager**. Quando si avvia il sistema per la prima volta, verranno richieste un ID supervisore e la password, come illustrato in basso.

Prima Esecuzione del Sistema di Accesso
Esegui il sistema di accesso per la prima volta.
Prego inviare ID Supervisore,Password.
ID :
Password :
Password Confirmation :
Suggerimento :
Auto Login:
Per memorizzare questa ID e password, e per fare il login quando esegui il sistema di accesso ogni volta.
Permetti rimozione password di sistema
OK
Cancella

Figura 2-1

Inserire il nome desiderato per il supervisore nel campo ID. Terminare l'impostazione inserendo Password, Password Confirmation e Suggerimento (opzionale) per ricordare la password. Funzioni disponibili nella finestra di dialogo:

- **Auto Login:** permette l'acceso automatico dell'utente corrente ogni volta che viene lanciato il sistema. Per motivi di sicurezza, questa funzione è consigliata solo per sistemi con un singolo utente.
- **Permetti rimozione password di sistema:** permette all'utente di rimuovere il database di ID e password dal sistema. È consigliabile verificare questa opzione in caso di perdita della password. Per i dettagli vedere la stessa opzione nella figura 7-1.
- **:** Fare clic su questa icona per aprire la tastiera a schermo e inserire le informazioni di login.

Fare clic su **OK** e andare alla schermata principale di ASManager.

Capitolo 3 La schermata principale di ASManager

Una volta eseguito ASManager, verrà visualizzata la seguente schermata principale. Familiarizzare con la schermata principale, perché sarà utile per la lettura delle sezioni successive.

3.1 Schermata principale

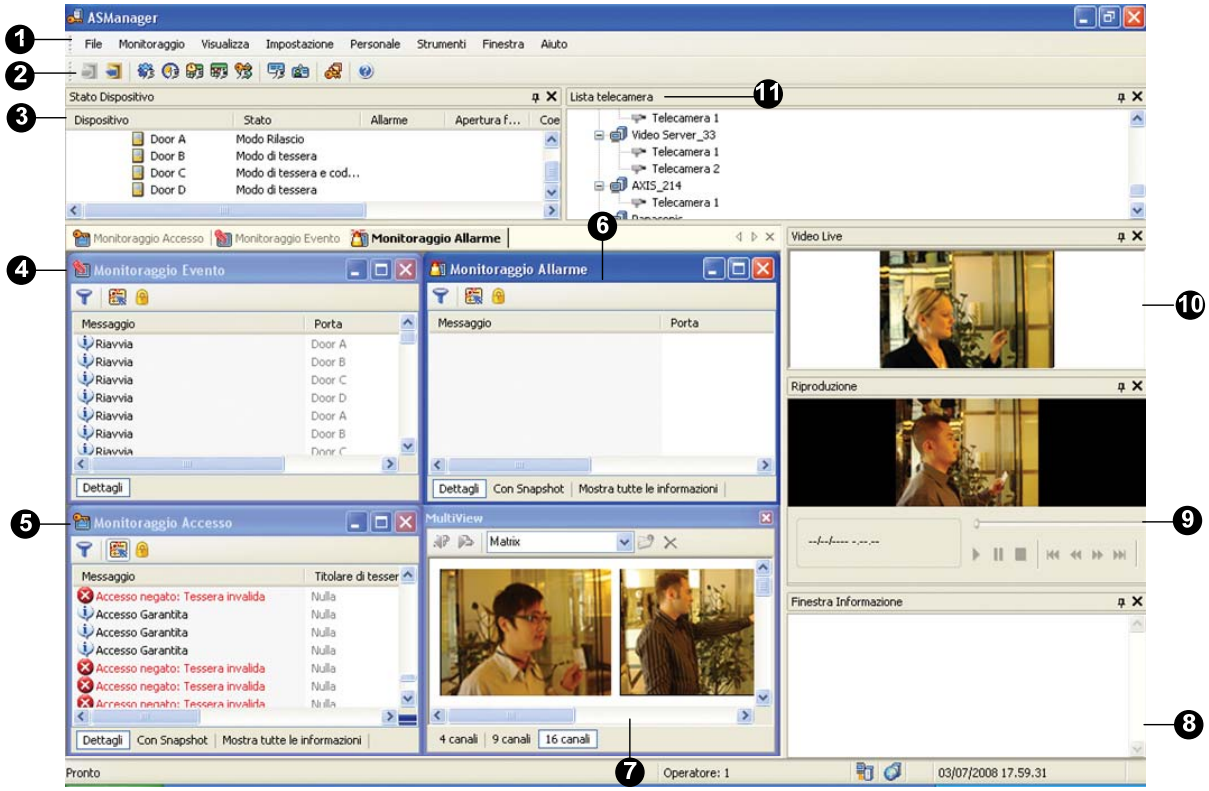


Figura 3-1

N.	Nome	Funzione
1	Barra dei menu	La barra dei menu include le opzioni di **File** (accesso/uscita da ASManager), **Monitoraggio** (visualizzazione delle finestre di allarme, accesso ed evento), **Visualizza** (visualizzazione delle finestre delle funzioni), **Impostazione** (impostazione dei dispositivi connessi e delle programmazioni), **Personale** (impostazione degli account dei titolari di tessere) e **Finestra** (organizza la visualizzazione di diverse finestre).

2	Barra degli strumenti	La barra degli strumenti include le opzioni di **Login, Logout, Dispositivi, Fuso orario, Schedulazione settimanale, Ferie, Gruppi di accesso, Tessere, Titolari di tessera, ASLog** e **Informazioni**.
3	Stato Dispositivo	Visualizza un elenco di porte connesse e il loro stato corrente.
4	Monitoraggio Evento	Visualizza gli eventi monitorati delle porte.
5	Monitoraggio Accesso	Visualizza le attività di accesso delle porte.
6	Monitoraggio Allarme	Visualizza gli eventi di allarme delle porte.
7	MultiView	Visualizza le viste live delle telecamere connesse da diversi dispositivi IP. Per i dettagli vedere "La finestra MultiView" nel Capitolo 5.
8	Finestra Informazione	Visualizza le informazioni sulle porte, sui lettori e sugli eventi monitorati.
9	Riproduzione	Riproduce gli eventi registrati da un dispositivo IP GeoVision compatibile. Per i dettagli vedere "Recupero video registrati" nel Capitolo 5.
10	Video Live	Visualizza la vista live di una delle telecamere connesse. Per i dettagli vedere "Accesso alla visualizzazione live" nel Capitolo 5.
11	Lista telecamera	Visualizza un elenco di telecamere connesse.

3.1.1 Barra degli strumenti

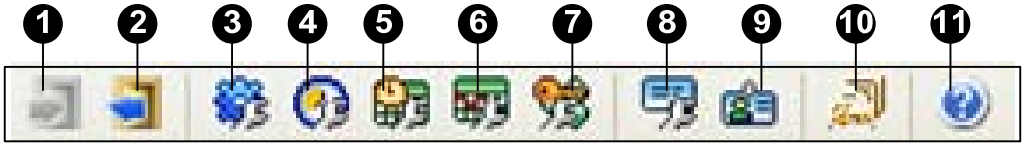


Figura 3-2

Tasti sulla barra degli strumenti di ASManager:

N.	Nome	Funzione
1	Login	Per accedere a ASManager.
2	Logout	Per uscire da ASManager.
3	Dispositivi	Definisce i controllori e le porte.

4	Fuso orario	Definisce i minuti e le ore del giorno durante le quali all'utente è consentito l'acceso ad un sito sicuro. Per i dettagli vedere "Impostazione del fuso orario" nel Capitolo 4.
5	Schedulazioni settimanali	Definisce i giorni della settimana durante i quali all'utente è consentito l'acceso ad un sito sicuro. Per i dettagli vedere "Impostazione delle schedulazioni settimanali" nel Capitolo 4.
6	Ferie	Definisce delle date specifiche come ferie. Per i dettagli vedere "Impostazione delle ferie" nel Capitolo 4.
7	Gruppo di accesso	Imposta i diversi gruppi per definire chi può accedere, da quale porta a quale ora del giorno. Per i dettagli vedere "Impostazione dei gruppi di accesso" nel Capitolo 4.
8	Tessere	Crea e modifica un database di informazioni sulle tessere. Per i dettagli vedere "Impostazione tessere" nel Capitolo 4.
9	Titolari delle tessere	Crea e modifica un database di informazioni sui titolari delle tessere. Per i dettagli vedere "Impostazione dei titolari delle tessere" nel Capitolo 4.
10	ASLog	Visualizza i registri delle attività di accesso, i rapporti di allarme e gli eventi monitorati. Per i dettagli vedere il Capitolo 6 *ASLog*.
11	Informazioni	Visualizza la versione di ASManager.

3.2 Stato dispositivo

Lo Stato dispositivo visualizza l'attività e lo stato delle porte connesse.

- Per aprire la finestra Stato dispositivo, fare clic su **Visualizza** sulla barra dei menu e selezionare **Stato Dispositivo**.

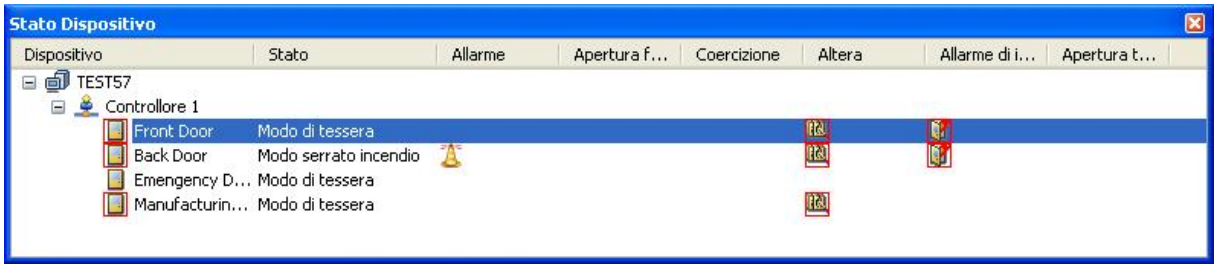


Figura 3-3

3.2.1 Controllori nella finestra

È possibile comandare un controllore o una porta connessa facendo clic con il tasto destro del mouse sulla finestra dello stato dispositivo.

Le opzioni del menu del controllore includono:

Nome	Funzione
Ripristina Anti-passback:	Facendo clic su questa opzione si abilita un utente a riaccedere al lettore in entrata prima di uscire. Vedere “Anti-Passback” nella Fase 2, sezione 4.2.2 della *Fase 2: Configurazione di una porta*.
Update	Una volta modificate le impostazioni del controllore, facendo clic immediatamente su Update si aggiornano le impostazioni.
Impostazioni	Modifica le impostazioni del controllore nella finestra di dialogo Impostazione di controllore.

Le opzioni del menu del controllore includono:

Nome	Funzione
Porta non serrata, Forza a non serrare, Forza a serrare, Disabilita l’operazione della porta serrata.	Controlla i comportamenti della porta.
Cancella allarme, Cancella apertura forzata, Cancella coercizione, Cancella alterazione, Cancella allarme di incendio, Cancella apertura tenuta, Cancellare accesso negato	Annulla gli allarmi sulla viasualizzazione del dispositivo. Per le impostazioni di allarme, vedere Fase 5 nella sezione 4.2.2 della *Fase 2: Configurazione di una porta*. Notare che Cancella allarme si riferisce all’annullamento dei segnali acustici di allarme.
Impostazioni	Modifica le impostazioni del controllore nella finestra di dialogo Impostazione di controllore.

3.3 Monitoraggio finestre

Gli utenti hanno a disposizione tre finestre di monitoraggio per sorvegliare diversi tipi di attività della porta: Monitoraggio accesso, Monitoraggio allarme e Monitoraggio evento.

- Per aprire queste finestre, fare clic su **Monitoraggio** sulla barra dei menu e selezionare le finestre desiderate.

3.3.1 Comandi all'interno della finestra

Le tre finestre di monitoraggio (Monitoraggio accesso, Monitoraggio allarme e Monitoraggio evento) al loro interno hanno gli stessi comandi.

Per spiegare i comandi usiamo come esempio la finestra Monitoraggio accesso.

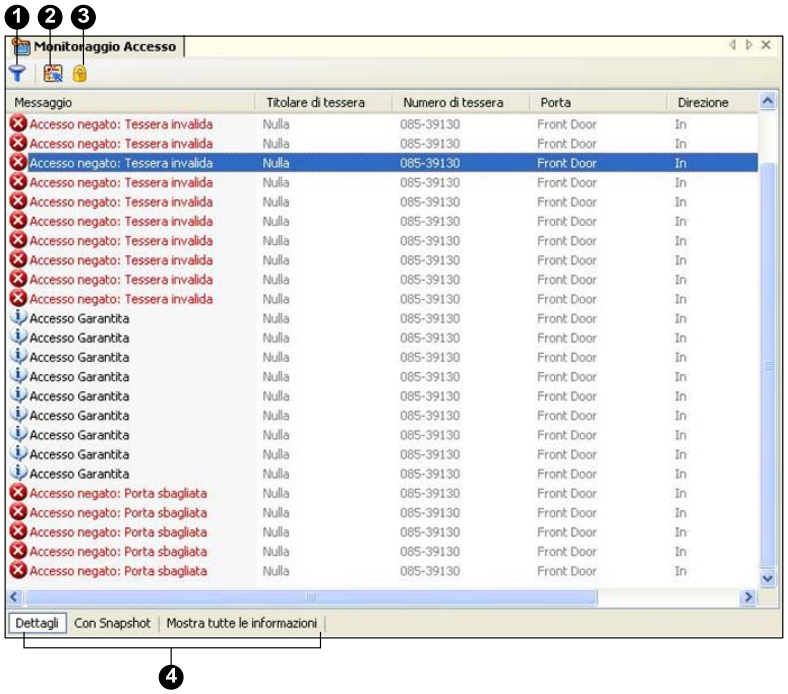


Figura 3-4

N.	Nome	Funzione
1	Filtro	Imposta i criteri per visualizzare solo le informazioni dell'attività desiderata.
2	Selezione automatica	Si concentra solo sulla visualizzazione dati più recente.
3	Serrare	Sospende la visualizzazione di dati corrente.
4	Dettagli / Con Snapshot / Mostra tutte le informazioni	Per decidere come visualizzare gli eventi nella finestra.

Facendo clic con il tasto destro del mouse sul messaggio della finestra, appare un menu opzionale per accedere alle informazioni dettagliate su questo messaggio.

- **Aggiungi/Modifica tessera:** registra una nuova tessera o ne modifica le informazioni.
- **Naviga informazione della tessera:** visualizza le informazioni contenute nella tessera.
- **Naviga informazione del titolare di tessera:** visualizza le informazioni del titolare della tessera.
- **Mostra immagine:** Se la videocamera era attiva quando si è verificata l'attività, sarà disponibile la relativa immagine.

3.3.2 Personalizzazione di una finestra di monitoraggio

È possibile personalizzare i messaggi visualizzati su una finestra di monitoraggio grazie alla definizione dei criteri di ricerca. In base ai requisiti specifici possono essere aggiunte finestre di monitoraggio personalizzate.

1. Per aggiungere una finestra di monitoraggio, fare clic su **Monitoraggio** sulla barra dei menu. Quindi selezionare **Nuovo monitoraggio allarme, Nuovo monitoraggio accesso** e **Nuovo monitoraggio evento**.
2. Fare clic sul tasto **Filtro** all'interno della finestra Monitoraggio. Appare questa finestra di dialogo.

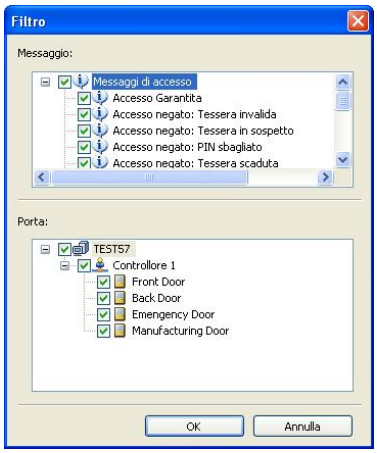


Figura 3-5

3. Selezionare i messaggi e i dispositivi desiderati per il monitoraggio quindi fare clic su **OK**. La finestra di monitoraggio visualizzerà solo i messaggi basati sui criteri definiti.
4. Fare clic con il tasto destro del mouse sulla scheda **Monitor** nella schermata principale e selezionare **Rinomina** per assegnare un nome alla nuova finestra di monitoraggio.

Figura 3-6

Nota: le finestre aggiunte possono essere utilizzate solo per un'unica sessione e non possono essere salvate alla chiusura di ASManager.

3.3.3 Organizzare le finestre di monitoraggio

Le finestre di monitoraggio possono essere organizzate sulla schermata in vari modi.

Sulla barra dei menu, fare clic su **Finestra** e selezionare una delle seguenti opzioni per organizzarle:

- **Cascata:** sovrappone le finestre aperte e ne mostra le barre del titolo.
- **Metti in orizzontale:** posiziona le finestre aperte in orizzontale.
- **Metti in verticale:** posiziona le finestre aperte in verticale.
- **Arrangia icone:** posiziona le finestre ridotte nella parte inferiore della schermata.

Se si impostano molte finestre di monitoraggio, è anche possibile fare clic su **Finestra** e selezionare **Più finestre** per visualizzare l'elenco completo delle finestre di monitoraggio.

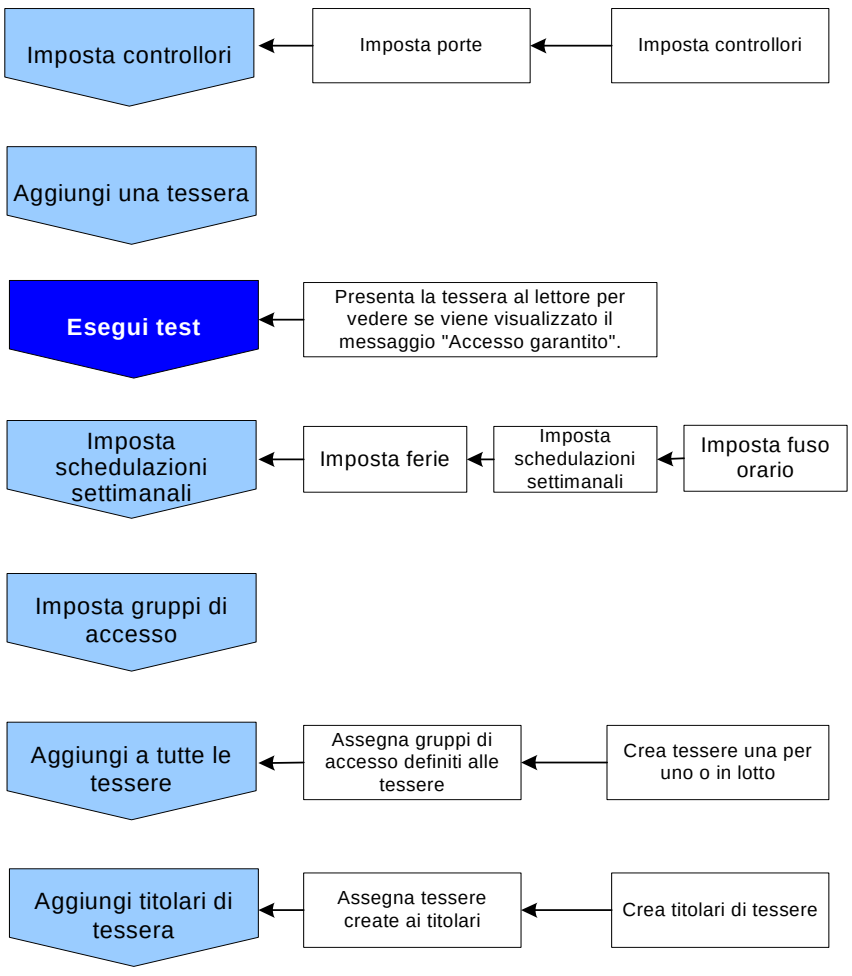
Capitolo 4 Impostazioni

Questa sezione descrive le seguenti impostazioni:

- Impostazione dei controllori
- Impostazione tessere
- Impostazione delle schedulazioni settimanali
- Impostazione gruppi di accesso
- Impostazione titolari di schede

4.1 Diagramma di flusso delle impostazioni

Per eseguire velocemente le impostazioni di ASManager, seguire la procedura illustrata in basso.


Imposta controllori
Imposta porte
Imposta controllori
Aggiungi una tessera
Esegui test
Presenta la tessera al lettore per vedere se viene visualizzato il messaggio "Accesso garantito".
Imposta schedulazioni settimanali
Imposta ferie
Imposta schedulazioni settimanali
Imposta fuso orario
Imposta gruppi di accesso
Aggiungi a tutte le tessere
Assegna gruppi di accesso definiti alle tessere
Crea tessere una per uno o in lotto
Aggiungi titolari di tessera
Assegna tessere create ai titolari
Crea titolari di tessere

4.2 Aggiungere controllori

Per aggiungere il controllore AS200 ad ASManager, seguire queste istruzioni:

- **Fase 1 Configurazione di un controllore per la porta**

  Stabilire la comunicazione fra il controllore AS200 e ASManager.

- **Fase 2 Configurare una porta**

  Definire le porte su un apposito controllore.

4.2.1 Fase 1: configurazione di un controllore per la porta

1. Sulla barra dei menu, fare clic su **Impostazione** e selezionare **Dispositivo**. Appare la finestra di dialogo Controller List (Elenco controllori).
2. Fare clic sull'icona **Aggiungi** nell'angolo in alto a sinistra. Appare questa finestra di dialogo.

Figura 4-1

3. Assegnare un **ID** e un **Nome** al controllore AS200 e fare clic su **OK**. Appare questa finestra di dialogo.

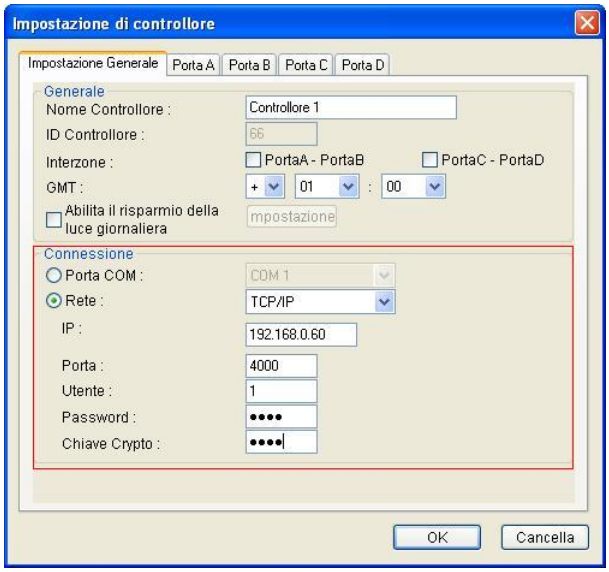


Figura 4-2

Nota: L'ID del Controller AS200 è stato impostato preventivamente con ASKeypad o con l'interfaccia di configurazione web. Fare riferimento a "5.2 Impostazione parametro" e "6.2.4 Impostazione ID del controllore e della modalità di lavoro" su *Guida all'installazione hardware del controllore AS200*.

---

4. Nella sezione Connessione, selezionare la modalità di comunicazione fra il controllore AS200 e ASManager.
   - Se si usa una connessione RS-485, selezionare la **Porta COM** usata per la connessione.
   - Se si usa la rete Ethernet, selezionare **Rete** e quindi **TCP/IP** o **LocalDDNS**. Digitare indirizzo IP, nome dispositivo (se è selezionato LocalDDNS), numero porta, utente login, password login e chiave di criptazione (codice 3DES) del controllore AS200.
5. Impostazioni OPZIONALI nella sezione Generale:
   - **Interzone:** abilitare la funzione di "interlocking" fra due porte (porta A e porta B, oppure porta C e porta D). Le porte interbloccate non possono essere aperte contemporaneamente. Una porta si sblocca solo quando l'altra è chiusa.
   - **GMT:** l'ora corrente sul computer host.
   - **Abilita il risparmio della luce giornaliera:** abilitare la funzione di risparmio della luce. Il sistema regolerà automaticamente il tempo di risparmio della luce.

Nota: i valori predefiniti del controllore sono: indirizzo IP **192.168.0.100**; nome utente **admin**; password **1234**; chiave di criptazione (codice 3DES) **12345678**. Per i dettagli sulle impostazioni del controllore AS200, vedere *Guida all'installazione hardware del controllore AS200*.

4.2.2 Fase 2: configurare una porta

1. Per definire le porte sul controllore, fare clic sulla scheda **Porta** (porta A, B, C, o D). Appare questa finestra di dialogo.

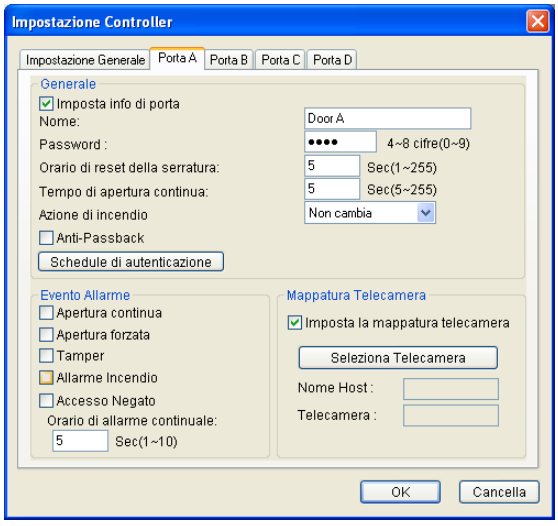


Figura 4-3

2. Nella sezione Generale, abilitare **Imposta info di porta** per definire i parametri generali della porta:

   - **Nome:** assegnare un nome alla porta.
   - **Password:** assegnare una password alla porta. L'impostazione predefinita è 1234.
   - **Orario di reset della serratura:** Se la porta è controllata, inserire il numero di secondi per cui essa deve rimanere aperta. Una volta scaduto il tempo specificato, la porta si chiuderà automaticamente.
   - **Tempo di apertura continua:** Se la porta è controllata, inserire il numero di secondi per cui essa deve rimanere aperta prima che venga generato un allarme per porta tenuta aperta.
   - **Azione di incendio:** regolare la porta come aperta o chiusa, nel caso si verifichi un allarme antincendio.
   - **Anti-passback:** Se è abilitata un'opzione anti-passback, una scheda usata su una porta di accesso non può essere usata di nuovo sulla stessa porta, a meno che non la si utilizzi su una corrispondente porta di uscita. Ciò è applicabile alle modalità di lavoro **Traffico a senso unico** e **Controllo a doppio senso**.

3. Per definire la modalità di accesso, fare clic sul tasto **Schedule di autenticazione**. Appare questa finestra di dialogo.

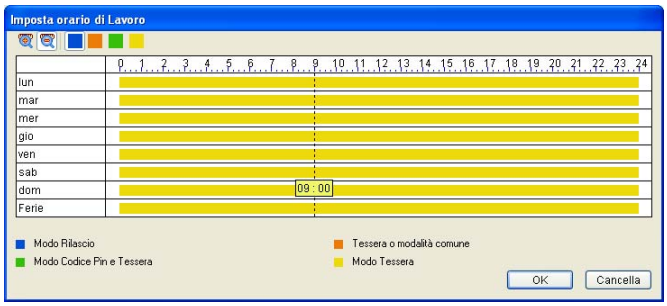


Figura 4-4

4. Per definire che tipo di modalità di accesso deve essere applicata in un giorno e in un orario specifico, selezionare una modalità di accesso sulla barra degli strumenti e trascinare il mouse sulle sequenze cronologiche. Nel sistema sono disponibili quattro (4) modalità di accesso:

   - **Modo Tessera:** È la modalità predefinita. Richiede esclusivamente che l'utente presenti la sua scheda per ottenere l'accesso.
   - **Modo Rilascio:** Per mantenere la porta in uno stato di sblocco con il lettore.
   - **Modo Codice PIN e Tessera:** Questa modalità richiede che l'utente presenti la sua scheda e che immetta il PIN tramite la tastiera.

- **Tessera o modalità comune o :** Questa modalità richiede che l'utente presenti la sua scheda in modo che gli venga garantito l'accesso **OPPURE** che immetta la password della porta usando la tastiera.

5. Le impostazioni nella sezione Evento allarme sono OPZIONALI, a meno che sul controllore AS200 non sia installato un dispositivo di allarme. Abilitare le condizioni al cui verificarsi scatterà l'allarme: **Apertura tenuta, Apertura forzata, Manomissione, Allarme antincendio** e **Accesso negato**.

   - **Orario di allarme continuato:** inserire il numero di secondi per cui deve durare l'allarme.

6. Le impostazioni nella sezione Mappatura telecamera sono OPZIONALI, a meno che non ci sia una videocamera installata nel sito sicuro. Per i dettagli vedere il *Capitolo* 5 *Integrazione video*.

7. Fare clic su **OK** più volte e tornare alla schermata principale. Nella finestra Stato dispositivo apparirà una struttura ad albero del controllore, come illustrato nell'esempio in basso.

   Se appare l'icona , significa che è stata stabilita la connessione fra il controllore e ASManager.

   Se appare l'icona , significa che la connessione non è riuscita. Accertarsi che l'impostazione della connessione di cui sopra sia configurata correttamente.

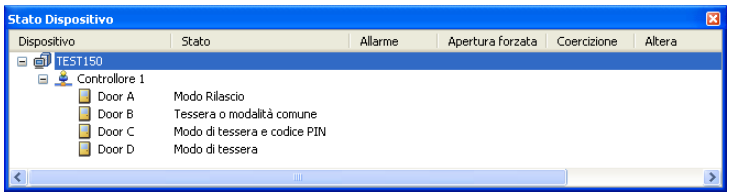


Figura 4-5

4.3 Impostazione tessere

Una volta configurato il controllore, è possibile iniziare la registrazione delle tessere. Tutte le nuove tessere devono essere registrate in ASManager, prima che sia consentito l'accesso. È possibile archiviare fino a 10.000 tessere in ASManager. Se sul lettore viene presentata una tessera non registrata, apparirà il messaggio *Accesso negato: tessera invalida*.

A seconda del numero di tessere che si necessita programmare, è possibile aggiungerle una alla volta o usare la funzione batch per aggiungere un gruppo di schede.

4.3.1 Aggiungere una singola scheda

1. Per aggiungere una scheda, seguire uno di questi metodi:

   - Presentare la scheda al lettore. È visualizzato il messaggio *Accesso negato: Scheda non valida.* Fare clic con il tasto destro del mouse sul messaggio e selezionare **Crea/Modifica tessera**. Viene visualizzata la finestra di dialogo Nuova tessera con il numero della scheda e il tipo codice inserito (vedere Figura 4-7). Quindi, per completare le altre impostazioni, seguire la Fase 3.

   - Sulla barra dei menu, fare clic su **Personale** e selezionare **Tessere**. Appare questa finestra.

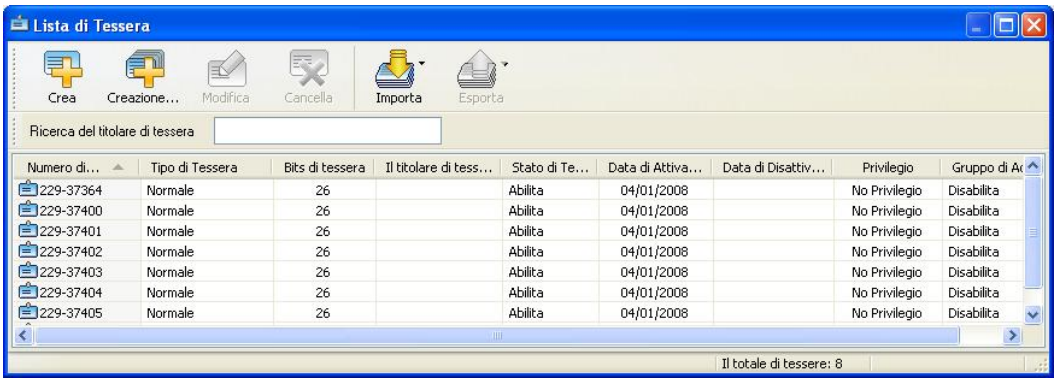

Lista di Tessera
Crea
Creazione...
Modifica
Cancella
Importa
Esporta
Ricerca del titolare di tessera
Numero di...
Tipo di Tessera
Bits di tessera
Il titolare di tess...
Stato di Te...
Data di Attiva...
Data di Disattiv...
Privilegio
Gruppo di Ac
229-37364 Normale 26 Abilita 04/01/2008 No Privilegio Disabilita
229-37400 Normale 26 Abilita 04/01/2008 No Privilegio Disabilita
229-37401 Normale 26 Abilita 04/01/2008 No Privilegio Disabilita
229-37402 Normale 26 Abilita 04/01/2008 No Privilegio Disabilita
229-37403 Normale 26 Abilita 04/01/2008 No Privilegio Disabilita
229-37404 Normale 26 Abilita 04/01/2008 No Privilegio Disabilita
229-37405 Normale 26 Abilita 04/01/2008 No Privilegio Disabilita
Il totale di tessere: 8

Figura 4-6

2. Fare clic sul pulsante **Crea** sulla barra degli strumenti. Appare questa finestra di dialogo.

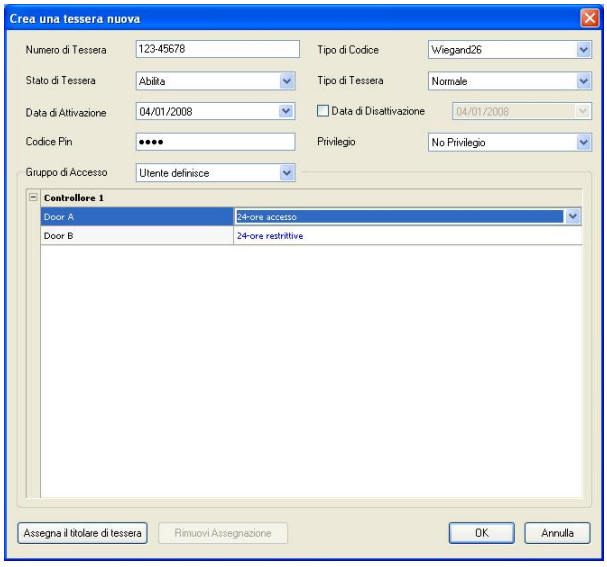


Figura 4-7

3. Per la scheda sono disponibili altre impostazioni:

   - **Numero di Tessera:** Inserire il numero della scheda.
   - **Tipo di Codice:** selezionare il formato di codice della scheda.

- **Tipo di Tessera:**
  - **Ronda:** La scheda è stata assegnata alla persona incaricata di sorvegliare il luogo, es. la guardia. Quando la scheda di tipo ronda, è presentata al lettore, l'accesso verrà registrato ma la porta non si sbloccherà. La funzione può essere impostata insieme al **Privilegio** in basso. L'utente può avere il privilegio di spegnere gli allarmi acustici e cancellare gli allarmi durante la sorveglianza.
  - **Tessera due persone A:** regola delle due persone A/B. Per sbloccare la porta su cui è applicata la regola delle due persone, è necessario presentare la tessera definita come A e l'altra tessera B.
  - **Tessera due persone B:** regola delle due persone A/B. Per sbloccare la porta su cui è applicata la regola delle due persone, è necessario presentare la tessera definita come B e l'altra tessera A.
- **Data di Attivazione/Disattivazione:** per specificare quando la tessera è attiva o disattiva.
- **Codice PIN:** inserire un codice personale a quattro cifre per la tessera. L'impostazione predefinita è 1234.
- **Privilegio:** per assegnare uno di questi privilegi al titolare di tessera:
  - **Arresta allarme:** Il titolare della tessera può arrestare l'allarme presentando la tessera.
  - **Cancella evento:** Il titolare della tessera può cancellare l'allarme presentando la tessera. Tutti gli allarmi nella finestra di visualizzazione del dispositivo vengono cancellati. Viene comunque mantenuta una registrazione di tali allarmi in Monitoraggio allarme.
- **Gruppo di Accesso:** Il comando Gruppo di accesso controlla il personale che può accedere, a quale porta e a quale ora. Per i dettagli vedere *4.5 Creazione di un gruppo di accesso.*
- Al primo utilizzo di ASManager il gruppo di accesso non è ancora stabilito. Selezionare **Utente definisce** per eseguire il test.
- **Controllore:** La colonna Controllore visualizza le porte associate. Quando si inserisce un gruppo di accesso, la selezione per ogni porta appare automaticamente.
- Al primo utilizzo di ASManager, per eseguire il test selezionare **24-ore accesso**.

4. Presentare la tessera registrata al lettore. Una volta accettata la tessera, apparirà il messaggio *Accesso garantito*.

4.3.2 Aggiungere un gruppo di tessere

Prima di usare la funzione Batch per registrare nuove tessere, notare che i gruppi di schede devono essere numerati in sequenza.

1. Sulla barra dei menu, fare clic su **Personale** e selezionare **Tessere**. Appare la finestra di dialogo Lista di tessera.
2. Fare clic sul pulsante **Nuovo lotto** sulla barra degli strumenti. Appare questa finestra di dialogo.

Figura 4-8

3. Le impostazioni nelle finestra di dialogo sono le stesse di quelle per aggiungere una singola scheda. Vedere *Aggiungere una singola scheda*.

Nota: le schede registrate con la funzione Batch avranno lo stesso PIN. Se si desidera cambiare il PIN di alcune schede, è necessario inserirlo usando la funzione **Modifica** nella finestra di dialogo Lista di tessera.

4.3.3 Importare/Esportare dati di tessere

I dati delle tessere possono essere esportati in formato mdb o xls.

Per esportare i dati delle schede:

1. Nella finestra Lista di tessera (vedere figura 4-6) selezionare le schede desiderate usando Ctrl + tasto sinistro del mouse.
2. Fare clic sul tasto **Esporta** e selezionare una di queste opzioni: **Esporta su Access** o **su Excel**.
3. Assegnare il percorso file ed eventualmente inserire una password per esportare i dati contenuti nella tessera.,

---

Nota: Il formato file Excel non supporta la protezione password.

Per importare i dati delle schede:

1. Nella finestra Lista di tessera (vedere figura 4-6), fare clic sul tasto **Importa** e selezionare una di queste opzioni: **Importa da Access** o **Importa da Excel**.
2. Assegnare il percorso file e inserire la **Password** se necessario. Fare clic su **OK**. Appare questa finestra di dialogo.

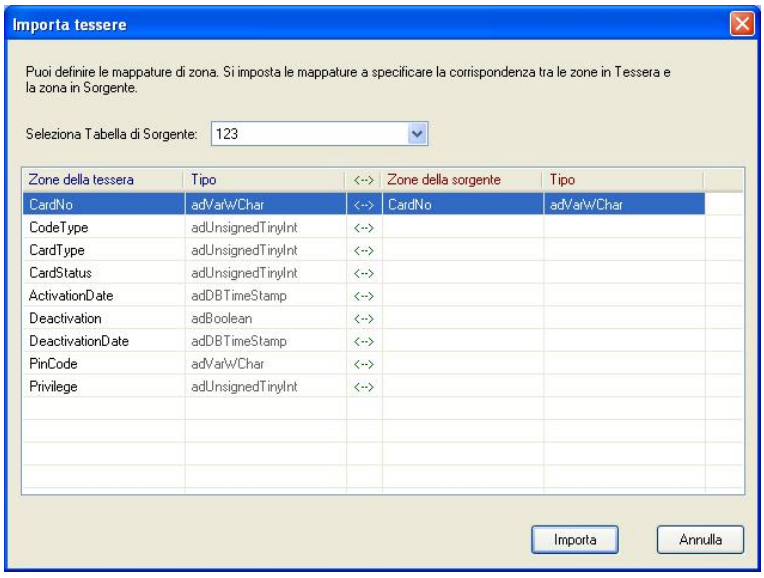


Figura 4-9

3. Selezionare **Tabella di sorgente** e fra clic sulle colonne sotto **Zone della sorgente** per abilitare la selezione. Selezionare i termini sorgente corrispondenti per mappare fra Zone della sorgente e Zone della tessera.
4. Fare clic su **Importa** per importare i dati della tessera.

4.4 Impostazione delle Schedulazioni Settimanali

Questa sezione aiuterà a definire i tempi di accesso giornalieri e delle ferie. È possibile definire fino a 254 schedulazioni settimanali con due programmi predefiniti per schedulazioni settimanali “nega accesso” e “accesso completo”.

Prima di creare la schedulazione settimanale, è utile mappare tutti gli usi possibili dei programmi settimanali per il sito. Ad esempio: considerare la varietà di orari di accesso dei dipendenti, i requisiti per il personale di sorveglianza che può avere bisogno di accedere, i requisiti per il personale di assistenza o addetto alla manutenzione che può avere bisogno di accesso a tutte le ore, i requisiti per lo staff di supervisione che può avere bisogno di un orario di accesso esteso, ecc.

- **Fase 1 Impostazione fuso orario**

  Definire i minuti e le ore del giorno durante le quali all’utente è consentito l’acceso ad un sito sicuro. Il tempo minimo è 5 minuti.

- **Fase 2 Impostazione schedulazioni settimanali**

  Definire i giorni della settimana durante i quali all’utente è consentito l’acceso ad un sito sicuro.

- **Fase 3 Impostazione ferie**

  Definire delle date specifiche come ferie.

4.4.1 Fase 1: Impostazione fuso orario

Questa sezione fornisce degli esempi per impostare i seguenti fusi orari:

- Orario diurno – dalle 09:00 alle 19:00
- Orario notturno – dalle 19:00 alle 9:00 (incrocio della mezzanotte)
- Supervisore – dalle 07:00 alle 24:00

1. Sulla barra dei menu, fare clic su **Configura** e selezionare **Fuso orario**. Appare questa finestra di dialogo.

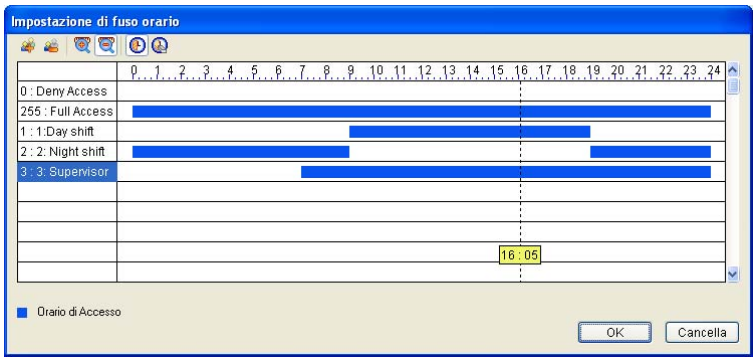

Impostazione di fuso orario
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
0 : Deny Access
255 : Full Access
1 : 1:Day shift
2 : 2: Night shift
3 : 3: Supervisor
16 : 05
Orario di Accesso
OK
Cancella

Figura 4-10

2. Fare clic sul tasto **Aggiungi** . Appare questa finestra di dialogo.

Figura 4-11

3. L'**ID** è il numero del fuso orario. Il sistema creerà automaticamente l'ID sulla base del numero di fusi orari aggiunti. Assegnare un **Nome** al fuso orario che si sta per definire. Fare clic su **OK**.

   Ad esempio, denominare il Fuso orario 1 **Orario diurno**.

4. Fare clic sul tasto **Aggiungi ora di accesso** . Quindi trascinare il mouse sulla sequenza cronologica per definire il periodo di accesso.

   Ad esempio, l'orario del turno diurno è **dalle 09:00 alle 19:00**.

5. Per creare il secondo fuso orario, fare clic sul tasto **Aggiungi** e assegnargli il nome di **Orario notturno**. Quindi fare clic sul tasto **Aggiungi ora di accesso** . Trascinare il mouse sulla sequenza cronologica per impostare l'ora **dalle 19:00 alle 24:00 e dalle 00:00 alle 9:00**.

6. Per creare il terzo fuso orario, fare clic sul tasto **Aggiungi** e assegnargli il nome di **Supervisore**. Quindi fare clic sul tasto **Aggiungi ora di accesso** . Trascinare il mouse sulla sequenza cronologica per impostare l'ora **dalle 07:00 alle 24:00**.

7. Fare clic su **OK**. I tre fusi orari sono stati definiti.

4.4.2 Fase 2: Impostazione delle Schedulazioni Settimanali

Questa sezione fornisce degli esempi per impostare le seguenti schedulazioni settimanali:

- Pianificazione - Orario diurno: dal lunedì al venerdì, dalle 09:00 alle 19:00.
- Pianificazione - Orario notturno: dal lunedì al venerdì, dalle 19:00 alle 09:00.
- Pianificazione - Supervisore: dal lunedì al sabato e festivi, dalle 07:00 alle 24:00.

1. Sulla barra dei menu, fare clic su **Impostazione** e selezionare **Schedulazioni settimanali**. Appare questa finestra di dialogo.

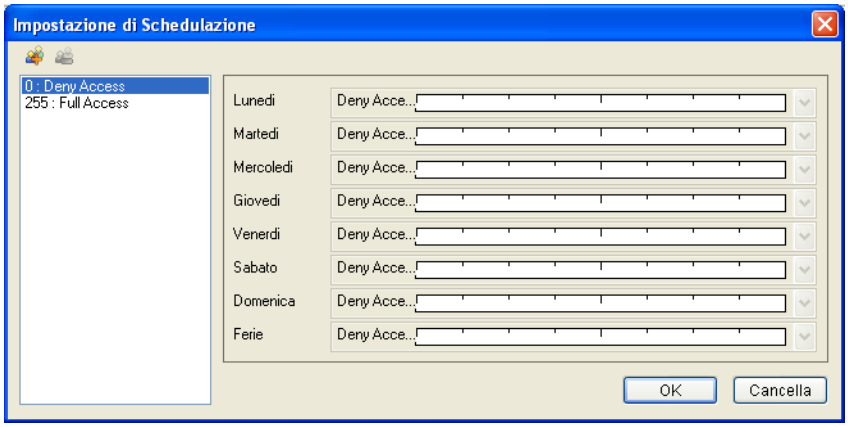


Figura 4-12

2. Cliccare sul tasto **Aggiungi**. Appare questa finestra di dialogo.

Figura 4-13

3. L'**ID** è il numero della schedulazione settimanale. Il sistema creerà automaticamente l'ID sulla base del numero di schedulazioni aggiunte. Assegnare un **Nome** alla schedulazione settimanale che si sta per definire. Fare clic su **OK**.

   Ad esempio, denominare la schedulazione settimanale 1 **Pianificazione - Orario diurno**.

4. Dagli elenchi a discesa da **Lunedì** a **Venerdì**, selezionare il fuso orario **Orario diurno** creato. Non è consentito l'accesso il sabato, la domenica e in occasione delle ferie.

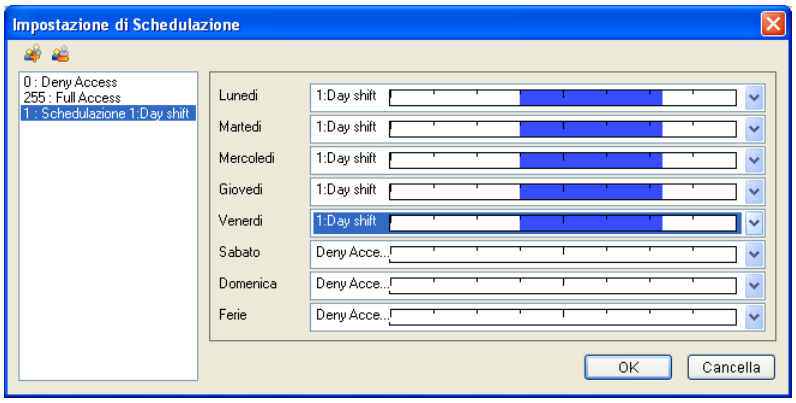


Figura 4-14

5. Per creare la seconda schedulazione, fare clic sul tasto **Aggiungi** e assegnargli il nome di **Pianificazione - Orario notturno**. Dagli elenchi a discesa da **Lunedì** a **Venerdì**, selezionare il fuso orario **Orario notturno** creato. Non è consentito l'accesso il sabato, la domenica e in occasione delle ferie.

6. Per creare la terza schedulazione, fare clic sul tasto **Aggiungi** e assegnargli il nome di **Pianificazione - Supervisore**. Dagli elenchi a discesa da **Lunedì** a **Ferie**, selezionare il fuso orario **Supervisore** creato.

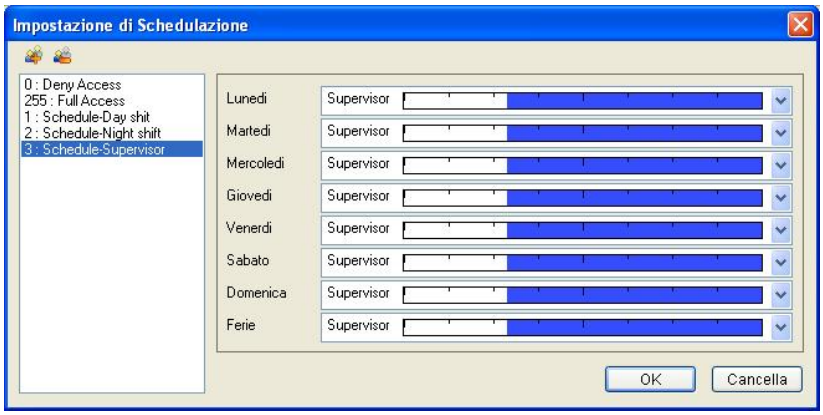


Figura 4-15

7. Fare clic su **OK**. Le tre schedulazioni settimanale sono state definite.

4.4.3 Fase 3: Impostazione delle ferie

Per indicare delle date specifiche come ferie sul sistema:

1. Sulla barra dei menu, fare clic su **Impostazione** e selezionare **Ferie**. Appare questa finestra di dialogo.

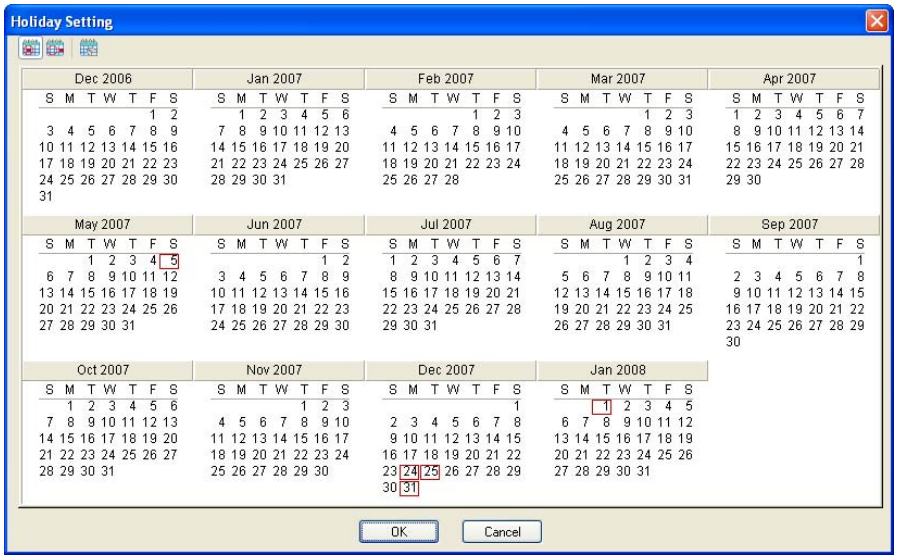


Figura 4-16

2. Fare clic sull'icona **Ferie** e sulle date specifiche di vacanza. Ad esempio:
   - 24 dicembre 2007 – Vigilia di Natale
   - 25 dicembre 2007 – Natale
   - 31 dicembre 2007 – San Silvestro
   - 1 gennaio 2008 - Capodanno
3. Per cancellare, fare clic sull'icona **Non festivo** e sulla data che si desidera eliminare.

Nota: le date delle ferie possono essere a cavallo dell'anno successivo, mentre alcune date variano di anno in anno. Gli amministratori devono esaminare e aggiornare l'impostazione delle ferie prima di iniziare un nuovo anno, per garantire una copertura adeguata delle vacanze.

4.5 Impostazione gruppi di accesso

I gruppi di accesso limitano il numero di persone che possono accedere, da quale porta e a quale ora. Perché gli sia garantito l'accesso ad una porta sicura, l'utente deve soddisfare i criteri del gruppo di accesso. L'utente si deve trovare presso una porta che accetta i membri di quel gruppo di accesso e nell'orario della schedulazione settimanale consentito.

Questa sezione utilizza un esempio per descrivere come creare un gruppo di accesso e assegnarne i criteri ad una tessera. In questo esempio, lo staff FAE addetto al turno diurno deve poter accedere alle porte anteriori e posteriori durante il giorno.

1. Sulla barra dei menu, fare clic su **Impostazioni** e selezionare **Access Groups (Gruppi di accesso)**. Appare questa finestra di dialogo.

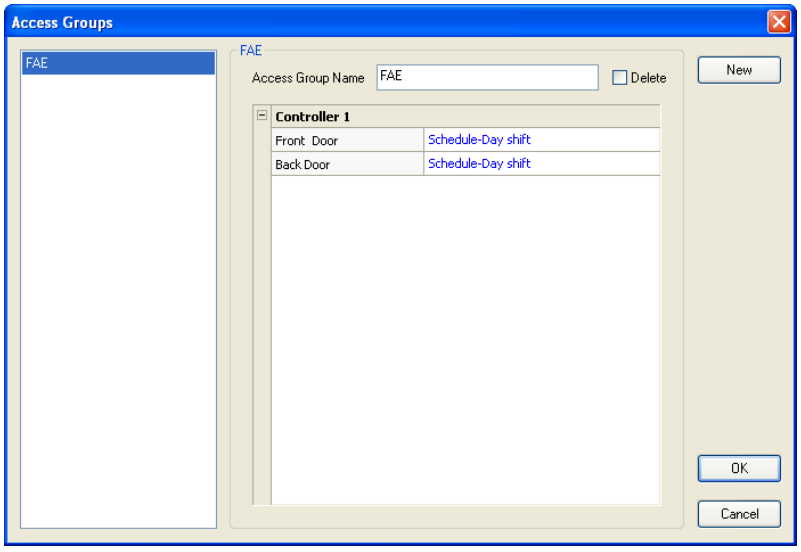


Figura 4-17

2. Fare clic sul tasto **New (Crea)** e assegnare un **Nome** al nuovo gruppo di accesso.

   Ad esempio, assegnare al gruppo il nome **FAE**.

3. Per definire l'accesso alle porte di questo gruppo, fare clic sull'elenco a discesa di ciascuna porta e selezionare una delle schedulazioni settimanali predefinite.

   Ad esempio, fare clic su ogni campo blu di **Porta anteriore e Porta posteriore**, quindi selezionare **Pianificazione - Orario diurno**.

4. Fare clic su **OK**. Il gruppo di accesso per lo staff FAE è stato creato.

5. Per assegnare i criteri del gruppo di accesso ad una singola tessera, fare clic su **Personale** sulla barra dei menu e selezionare **Tessere**. Appare la finestra di dialogo Lista di tessera.

6. Fare clic su una delle tessere nell'elenco. Appare questa finestra di dialogo.

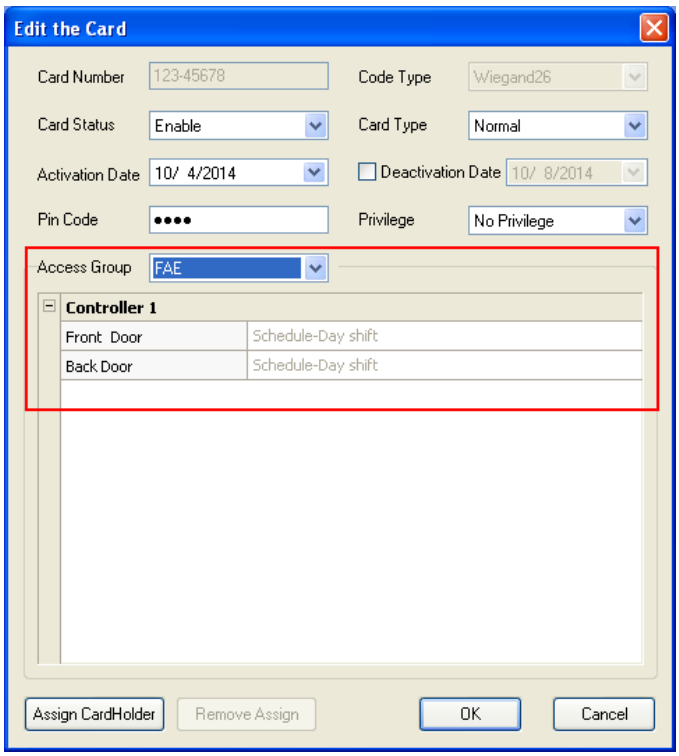


Figura 4-18

7. Dall'elenco a discesa **Gruppo di accesso** selezionare un gruppo di accesso predefinito, ad es. **FAE**. La schedulazione settimanale assegnata apparirà nel campo della porta associata.

4.6 Impostazione dei titolari di tessera

Questa sezione descrive come creare un database di informazioni sui titolari di tessera e assegnare le tessere ai titolari.

4.6.1 Aggiungere un titolare di tessera

1. Sulla barra dei menu, fare clic su **Personale** e selezionare **Titolari di tessera**. Viene visualizzata la finestra con l'Elenco dei titolari delle schede.
2. Fare clic sul pulsante **Nuovo** sulla barra degli strumenti. Appare questa finestra di dialogo.

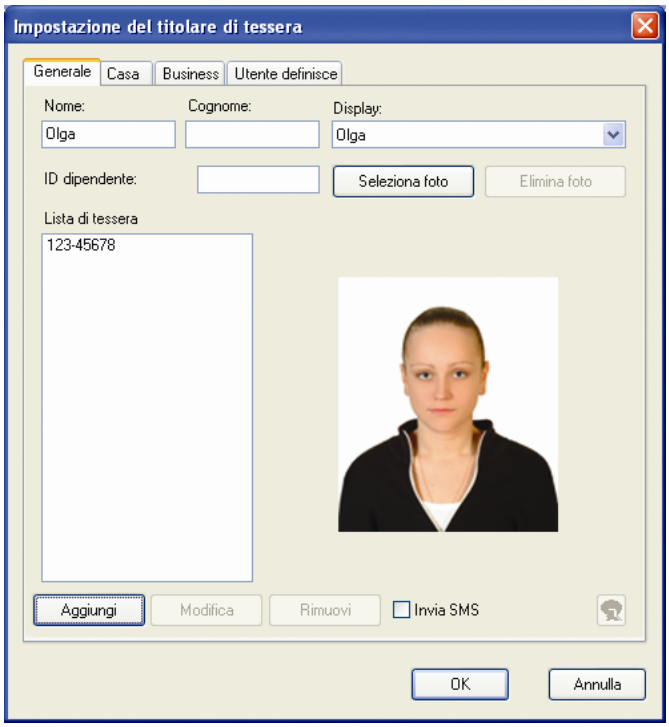


Figura 4-19

3. Inserire un Nome archiviato sotto **Display (Visualizza)**, come informazione minima. Altre informazioni sul titolare della scheda, come l'ID dipendente, la foto, le informazioni sull'abitazione e le informazioni sulla società, sono opzionali.

4.6.2 Assegnare una tessera ad un titolare

Ci sono due metodi per assegnare una tessera ad un titolare:

Nota: In questa fase, assumiamo che le istruzioni siano state seguite in *4.3 Impostazione delle schede* per completare la registrazione della scheda.

---

1. Nella finestra di dialogo Impostazione del titolare di tessera fare clic su **Aggiungi** per assegnare la/e tessera/e al titolare.
2. Nella finestra di dialogo Modifica (vedere Figura 4-18), selezionare **Assegna titolare** e fare doppio clic su un titolare di tessera elencato per eseguire tale operazione.

4.6.3 Invio allarmi SMS

Se si desidera inviare gli allarmi SMS ogni volta che le tessere assegnate al titolare vengono presentate al lettore, selezionare **Invia SMS** nella finestra di dialogo Impostazione titolare della scheda.

Prima di inviare l'SMS, vedere 7.2.1 *Impostazioni server SMS* per configurare il server SMS. Per le informazioni su come configurare gli avvisi SMS, fare riferimento alle stesse impostazioni "Invia allarme SMS" nella Fase 3 della sezione 7.2.3 di *Imposta notifica.*

4.6.4 Personalizzazione di un campo dati

È possibile personalizzare i campi dei dati dei titolari di tessere. Per ciascun inserimento di dati utente possono essere creati fino a dieci campi di dati.

Quando viene creato un campo dati personalizzato, l'etichetta del campo verrà visualizzata nella scheda Definito dall'utente nella finestra di dialogo Impostazione titolare della tessera. I dati personali reali di ciascun utente vengono immessi nella scheda Definito dall'utente.

Per personalizzare un campo dati:

1. Sulla barra dei menu, fare clic su **Personale** e selezionare **Titolari di tessera**. Viene visualizzata la finestra con l'elenco dei titolari di tessera.
2. Fare clic sul pulsante **Impostazione delle zone User Define** sulla barra degli strumenti. Viene visualizzata la finestra di dialogo Impostazione dei campi definiti dall'utente.
3. Selezionare un campo **Utente definisce**, e inserire il testo da visualizzare come etichetta del campo. In questo esempio è stata creato il campo di una targa automobilistica.

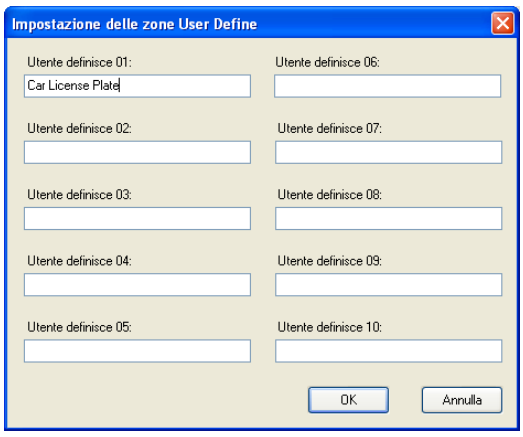


Figura 4-20

Per inserire dati personali:

1. Sulla barra dei menu, fare clic su **Personale** e selezionare **Titolari di tessera**. Viene visualizzata la finestra con l'elenco dei titolari di tessera.
2. Fare doppio clic su un utente elencato in cui devono essere inseriti dati personali. Si aprirà la finestra di dialogo Impostazioni titolare di tessera.
3. Fare clic sulla scheda **Utente definisce**. Viene visualizzato il campo dati personalizzato che è stato creato.
4. Fare clic sul campo dati personalizzato ed inserire le informazioni appropriate. In questo esempio viene inserito un numero nel campo creato Targa automobilistica.

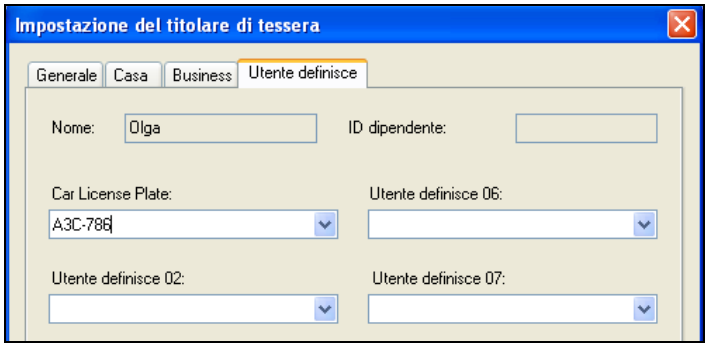


Figura 4-21

4.6.5 Importazione/Esportazione dei dati del titolare di tessera

Dalla finestra con l'Elenco dei titolari di tessera, è possibile importare ed esportare i dati del titolare in formato mdb o xls. Per questa funzione fare riferimento a *4.3.3 Importare/Esportare dati di schede*.

Capitolo 5 Integrazione video

I dispositivi IP GeoVision, e alcune telecamere IP di terze parti possono essere connessi a ASManager mediante la rete. È quindi possibile accedere ai video live a scopo di monitoraggio e sorveglianza.

ASManager fornisce le seguenti funzioni video:

- Visualizzazione live
- Riproduzione video
- Monitoraggio di 16 videocamere contemporaneamente

Nota:

- I dispositivi IP GeoVision includono GV-System, GV-NVR, GV-Video Server, GV-Compact DVR e GV-IP Camera. Per le telecamere IP compatibili di terze parti, vedere l'appendice.
- ASManager supporta solo GV-System della versione 8.120 o successiva.

Suggerimento: Nelle seguenti sezioni, il termine DVR fa riferimento al GV-System e GV-NVR, il termine "Video Server" fa riferimento a GV-Video Server, e il termine "Compact DVR" fa riferimento a "GV-Compact DVR.

5.1 Mappatura delle videocamere

Se si desidera mappare una telecamera dal DVR verso una porta, il DVR deve essere già stato abilitato per l'accesso video.

- Abilitare **Control Center Server** (CCS)

Per mappare una videocamera rispetto ad una porta:

1. Sulla barra dei menu, fare clic su **Impostazione** e selezionare **Dispositivo**. Appare la finestra di dialogo Controller List (Elenco controllori).
2. Fare doppio clic su un controllore nell'elenco. Si aprirà la finestra di dialogo Controller Setup (Impostazione di controllore).

3. Fare clic sulla scheda di una **Porta**. Appare questa finestra di dialogo.

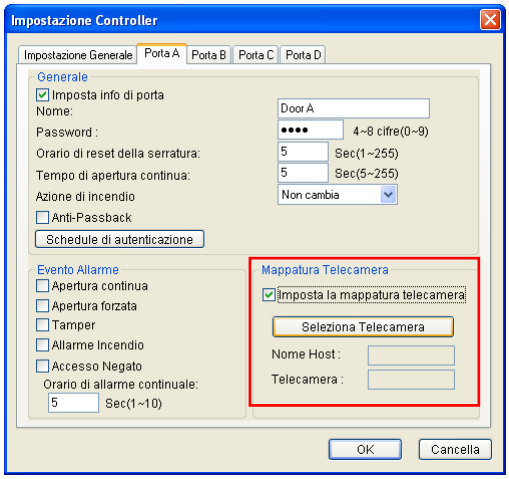


Figura 5-1

4. Nella sezione Mappatura telecamera, selezionare **Imposta la mappatura telecamera** e fare clic su **Seleziona Telecamera**. Appare questa finestra di dialogo.

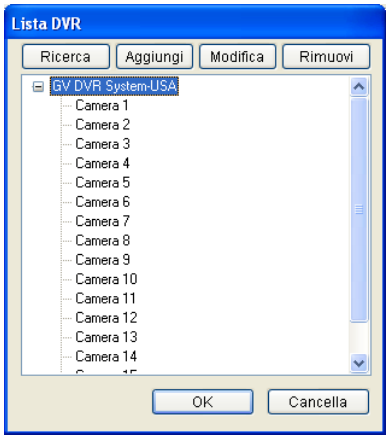


Figura 5-2

5. Per connettere un dispositivo IP a ASManager, usare uno dei seguenti metodi:

   - Fare clic su **Aggiungi**, selezionare il tipo di dispositivo IP e inserire l'indirizzo IP specifico.
   - Fare clic su **Ricerca** per rilevare tutti i dispositivi IP GeoVision sulla stessa LAN.

   Nelle istruzioni che seguono, come esempio, per stabilire il collegamento con un DVR viene utilizzato il primo metodo.

6. Fare clic su **Aggiungi**, quindi selezionare Aggiungi mappatura DVR per mappare una telecamera da un DVR alla porta.

7. Nella finestra di dialogo **Impostazione Host**, **Digitare Nome Host**, **Indirizzo IP**, **ID login** e **Password** del DVR.

8. Fare clic su **OK**. Il DVR verrà visualizzato nella finestra di dialogo dell'elenco DVR.

9. Ingrandire la cartella DVR, selezionare una videocamera e fare clic su **OK**. Il **Nome Host** e la **Videocamera** mappati sono visualizzati nella finestra di dialogo Impostazione di controllore.
10. Fare clic su **OK** più volte e tornare alla schermata principale.
11. Fare clic sulla porta specifica nella finestra Stato dispositivo. Viene visualizzata la vista live associata.

Nota: Se si utilizza la funzione **Ricerca** da aggiungere ai dispositivi IP GeoVision. È necessario fare clic sul tasto **Modifica** per inserirne gli ID e le password di registrazione, altrimenti non apparirà alcuna visualizzazione live.

5.2 Accesso a Vista live

Una volta effettuata la mappatura delle telecamere sulle porte, usare uno dei seguenti metodi per accedere alla visualizzazione live sulla finestra Live Video (vedere Figura 3-1).

- Nella finestra Stato dispositivo, fare clic sulla porta desiderata. Apparirà la visualizzazione live ad esso associato.
- Sulla finestra di Elenco telecamere, fare clic sulla telecamera desiderata. Apparirà la visualizzazione live ad esso associata.
- Nelle finestre Monitoraggio allarme e Monitoraggio accesso, fare clic sull'evento desiderato. Apparirà la visualizzazione live ad esso associata.

Per accedere alle viste live da più dispositivi IP, vedere *5.4 Finestra Multiview*, in basso.

5.3 Accedere all'immagine video

È possibile accedere all'immagine video degli eventi attivati da accesso e allarme.

- Nella finestra Monitoraggio allarme o Monitoraggio accesso, fare doppio clic sull'evento desiderato per visualizzare l'immagine. Oppure fare clic con il tasto destro del mouse sull'evento desiderato e selezionare **Mostra immagine** per visualizzare l'immagine. Notare che se non c'è nessuna immagine recuperabile, l'opzione verrà disattivata.

5.4 Finestra Multiview

La finestra MultiView fornisce una rapida panoramica in un'unica schermata di un massimo di sedici videocamere preimpostate. Queste telecamere possono essere un mix di telecamere di diversi dispositivi IP.

Per aprire e usare MultiView:

1. Sulla barra dei menu, fare clic su **Visualizzazione** e selezionare **MultiView**. Viene visualizzata la finestra MultiView, simile alla Figura 5-3.
2. Trascinare la videocamera desiderata dalla finestra Stato dispositivo o dall'elenco telecamere e rilasciarla nella necessaria cornice di Multiview.

Il video generato dalla telecamera viene visualizzato in questa cornice. Se già esiste una vista differente della telecamera in questa cornice, il nuovo video prende il suo posto.

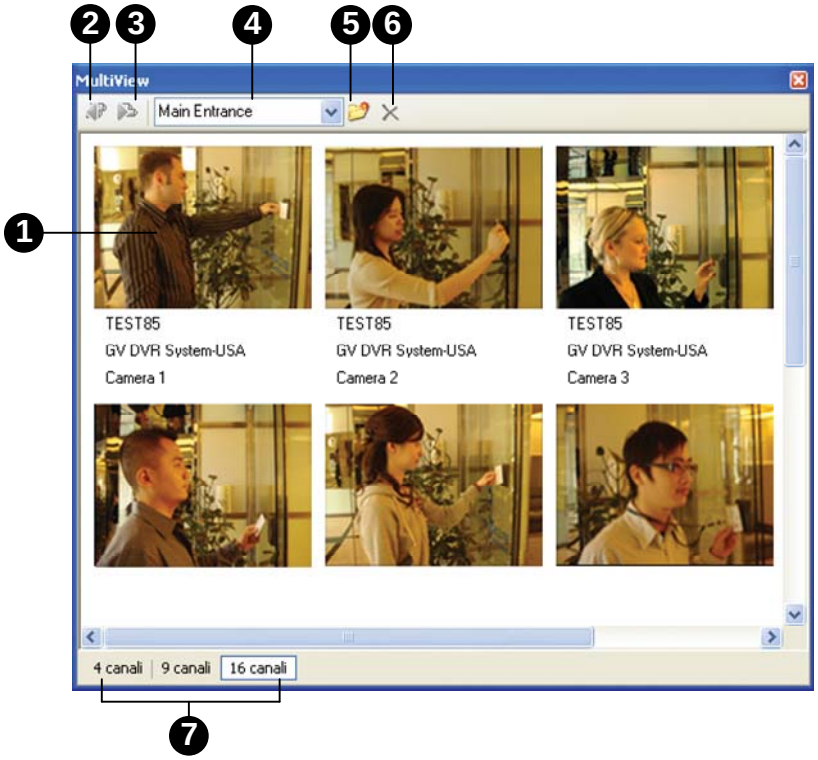


Figura 5-3

I controlli della finestra MultiView:

N.	Nome	Funzione
1	Cornice	Visualizza i video live della telecamera che vengono trascinati e rilasciati.
2	Pagina precedente	Va alla pagina precedente delle viste delle telecamere.
3	Pagina successiva	Va alla pagina successiva delle viste delle telecamere.
4	Visualizzazione a matrice	Selezionare una visualizzazione a matrice esistente (un gruppo di visualizzazioni) dall'elenco a discesa. Per i dettagli, vedere *5.4.1 Aggiunta di una visualizzazione a matrice.*
5	Aggiungi matrice	Aggiunge una visualizzazione a matrice.
6	Elimina matrice	Elimina una visualizzazione a matrice.
7	Visualizzazione canali	Visualizza 4, 9 o 16 canali sullo schermo.

Nota: È possibile trascinare la finestra Multiview all'esterno della schermata principale e anche sul monitor di un secondo computer.

5.4.1 Aggiunta di una visualizzazione a matrice

Una visualizzazione a matrice, o un gruppo di visualizzazioni, è una sistemazione programmata di cornici nella finestra MultiView che può presentare fino a sedici differenti visualizzazioni di telecamere. Le visualizzazioni a matrice multipla possono essere aggiunte come da necessità.

1. Nell'elenco a discesa Vista matrice, inserire un nome per la Vista matrice.
2. Cliccare sul tasto **Aggiungi matrice**. Il nome Vista matrice viene creato nell'elenco a discesa Vista matrice.
3. Trascinare la telecamera desiderata dalla Vista dispositivo o Elenco telecamera in una cornice disponibile della finestra. Il video associato alla telecamera viene visualizzato nella cornice.
4. È possibile ripetere le fasi da 1 a 3 per aggiungere più di una Vista a matrice. Quindi utilizzare l'elenco a discesa per passare a una differente Vista a matrice.

5.5 Recupero dei video registrati

I video registrati possono essere esaminati recuperandoli dal dispositivo IP GeoVision e riproducendoli. Prima di esaminare i video registrati sul dispositivo IP GeoVision, per avere l'accesso è necessario abilitare l'accesso remoto:

- DVR: abilitare **Remote ViewLog Service (Servizio remoto ViewLog)** su Control Center Server.
- Video Server, Compact DVR: abilitare la funzione **Remote ViewLog (ViewLog remoto)**.

Nota: GV-IP Camera non supporta la funzione di riproduzione.

Per riprodurre il video:

- Nella finestra Monitoraggio allarme o Monitoraggio accesso, fare clic sull'evento desiderato. Se esiste un video registrato, sarà abilitata la finestra Riproduzione. Fare clic sul tasto **Play** per riprodurre il filmato.

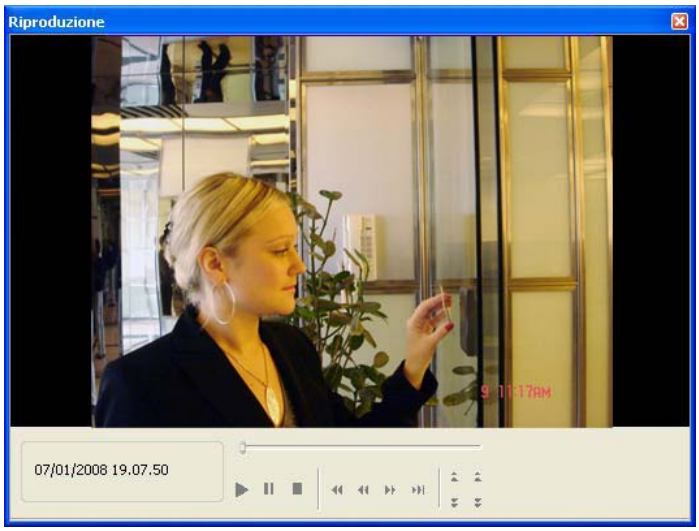
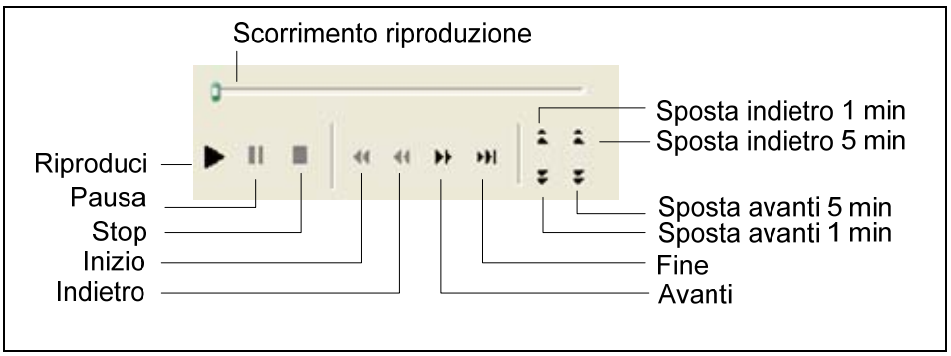


Figura 5-4



Fare clic con il tasto destro del mouse sulla finestra per rendere disponibili le seguenti funzioni:

Modo play	Include queste opzioni: • **Fotogramma per fotogramma:** riproduce il video fotogramma per fotogramma. • **Tempo reale:** riproduce il video in tempo reale. Questa modalità fa risparmiare il tempo necessario per il rendering, ma salta dei fotogrammi per rendere la riproduzione in tempo reale. • **Riproduzione automatica dei 5 minuti successivi:** riproduce il video fino a minuti. • **Audio:** attiva o disattiva l'audio.
Rendere	Include queste opzioni: • **Deinterlacciamento:** converte il video interlacciato in non interfacciato. • **Proporzionamento:** rende uniformi i quadrati del mosaico quando si ingrandisce un video riprodotto • **Sblocco:** rimuove gli artefatti tipo blocco da video di bassa qualità e molto compressi. • **Defog:** Migliora la visibilità dell'immagine. • **Stabilizzatore:** Riduce il tremolio della telecamera, • **Sovrapposizione nome videocamera e ora:** sovrappone al video il nome della videocamera e l'ora. • **Sovrapposizione POS/GV-Wiegand:** sovrappone al video i dati POS o GV-Wiegand Capture. • **Schermo intero:** Passa alla visualizzazione a schermo intero.
Strumenti	• **Snapshot:** Salva un'immagine video. • **Salva come AVI:** Salva un video in formato avi. • **Scarica:** Scarica i video clip da un dispositivo IP GeoVision nel computer locale.

Capitolo 6 ASLog

ASLog visualizza le informazioni sugli eventi delle porte durante la giornata corrente. I log vengono visualizzati con il messaggio di accesso, il nome del titolare della tessera, il numero di tessera, il nome delle porta e l'ora locale. È possibile anche accedere alle immagini e riprodurre il video, se disponibile.

Per visualizzare ASLog:

1. Per visualizzare ASlog, fare clic su **Strumenti** sulla barra dei menu e selezionare **ASLog**. Appare questa finestra.

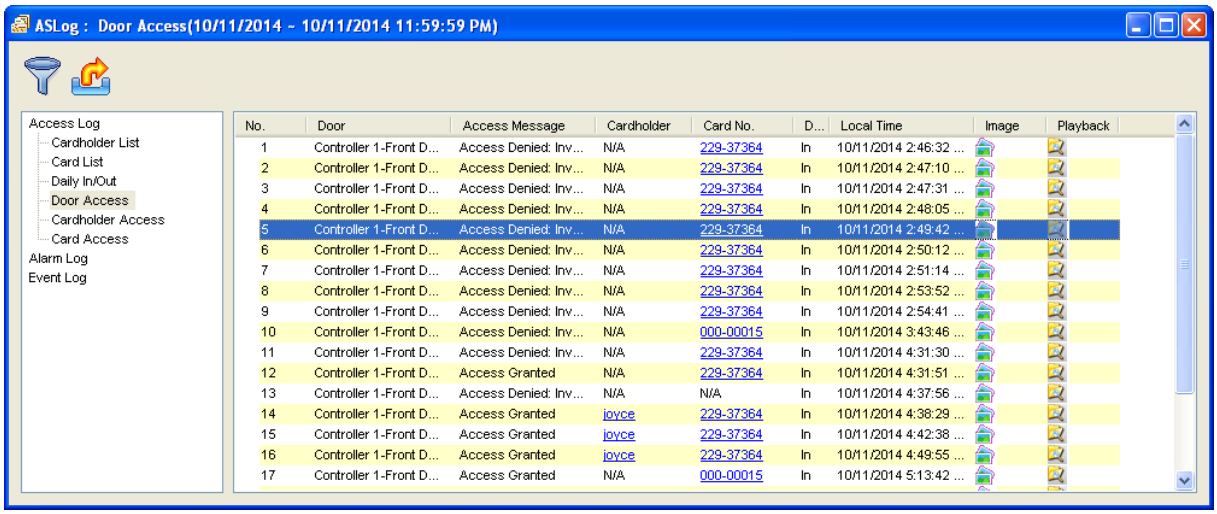

ASLog : Door Access(10/11/2014 ~ 10/11/2014 11:59:59 PM)
Access Log
Cardholder List
Card List
Daily In/Out
Door Access
Cardholder Access
Card Access
Alarm Log
Event Log
No. Door Access Message Cardholder Card No. D... Local Time Image Playback
1 Controller 1-Front D... Access Denied: Inv... N/A 229-37364 In 10/11/2014 2:46:32 ...
2 Controller 1-Front D... Access Denied: Inv... N/A 229-37364 In 10/11/2014 2:47:10 ...
3 Controller 1-Front D... Access Denied: Inv... N/A 229-37364 In 10/11/2014 2:47:31 ...
4 Controller 1-Front D... Access Denied: Inv... N/A 229-37364 In 10/11/2014 2:48:05 ...
5 Controller 1-Front D... Access Denied: Inv... N/A 229-37364 In 10/11/2014 2:49:42 ...
6 Controller 1-Front D... Access Denied: Inv... N/A 229-37364 In 10/11/2014 2:50:12 ...
7 Controller 1-Front D... Access Denied: Inv... N/A 229-37364 In 10/11/2014 2:51:14 ...
8 Controller 1-Front D... Access Denied: Inv... N/A 229-37364 In 10/11/2014 2:53:52 ...
9 Controller 1-Front D... Access Denied: Inv... N/A 229-37364 In 10/11/2014 2:54:41 ...
10 Controller 1-Front D... Access Denied: Inv... N/A 000-00015 In 10/11/2014 3:43:46 ...
11 Controller 1-Front D... Access Denied: Inv... N/A 229-37364 In 10/11/2014 4:31:30 ...
12 Controller 1-Front D... Access Granted N/A 229-37364 In 10/11/2014 4:31:51 ...
13 Controller 1-Front D... Access Denied: Inv... N/A N/A In 10/11/2014 4:37:56 ...
14 Controller 1-Front D... Access Granted joyce 229-37364 In 10/11/2014 4:38:29 ...
15 Controller 1-Front D... Access Granted joyce 229-37364 In 10/11/2014 4:42:38 ...
16 Controller 1-Front D... Access Granted joyce 229-37364 In 10/11/2014 4:49:55 ...
17 Controller 1-Front D... Access Granted N/A 000-00015 In 10/11/2014 5:13:42 ...

Figura 6-1

2. Dal riquadro a sinistra selezionare il criterio di raggruppamento, ad es. Accesso di porta. Gli eventi della giornata corrente appariranno in base alla selezione.
3. Per visualizzare i log dei giorni precedenti, fare clic sul tasto **Filtro**. Quindi definire i criteri di ricerca per individuare gli eventi desiderati.
4. Per esportare i risultati della ricerca, fare clic sul tasto **Esporta**. Salvare i risultati come file **.txt**, **.xls** o **.htm**.

Nota: È possible riprodurre il video solo quando il servizio remoto ViewLog incluso nel Control Center Server è abilitato nel DVR. E la funzione Viewlog remoto viene abilitata sul Video Server o sul Compact DVR.

Capitolo 7 Altre funzioni

7.1 Impostazione utente di sistema

L'utente del sistema è una persona che usa ASManager per monitorare i controllori delle porte, registrare i titolari di tessera o programmare il sistema. Mediante questa funzione, l'amministratore di sistema può creare nuovi utenti con diritti di accesso diversi. È possibile creare fino a 1.000 account utente.

7.1.1 Aggiungere un nuovo utente

1. Sulla barra dei menu, fare clic su **Strumenti** e selezionare **Account**. Appare questa finestra di dialogo.

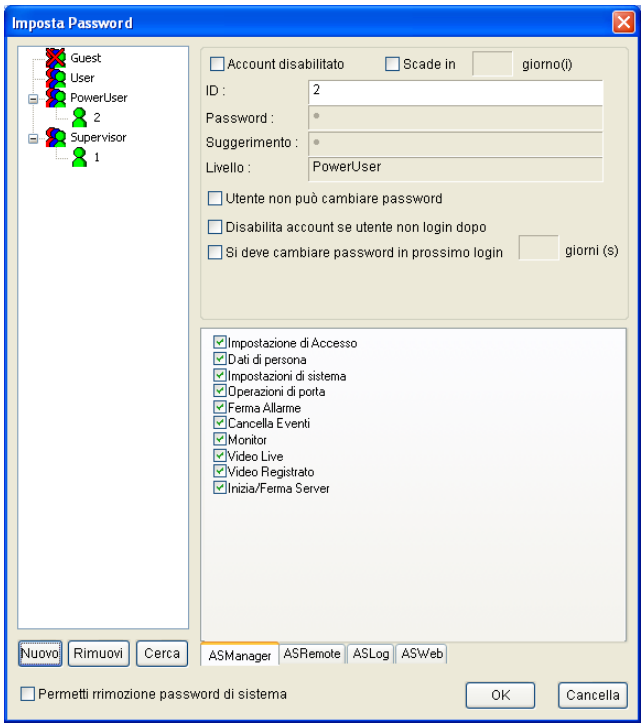


Figura 7-1

2. Fare clic su **Nuovo** nell'angolo in basso a sinistra. Appare questa finestra di dialogo.

Figura 7-2

3. Inserire **ID** utente e **Password**. Inserire di nuovo la stessa password nel campo Conferma password.
4. Fornire un **Suggerimento** (opzionale) per ricordare la password.
5. Selezionare il livello di autorizzazione dell'utente: **Supervisore**, **PowerUser** o **Utente**. Per impostazione predefinita, gli utenti appartenenti al livello Supervisore hanno tutti i diritti e le autorizzazioni per accedere alle impostazioni del sistema. I PowerUser hanno gli stessi diritti e le stesse autorizzazioni dei Supervisori, ad eccezione del fatto che non possono modificare le informazioni utente ed eliminare il sistema di password (descritto successivamente). Gli appartenenti al livello Utente non possono accedere alle impostazioni del sistema e hanno un accesso limitato a certe funzioni.
6. Fare clic su **OK** per aggiungere l'utente
7. Fare clic sulla scheda **ASManager**, **ASRemote**, **ASLog** o **ASWeb**

. Selezionare e deselezionare le funzioni autorizzate per l'utente.
8. Sono disponibili altre impostazioni:
   - **Scade in xx giorno(i):** l'account scadrà e sarà automaticamente disabilitato dopo un certo numero di giorni. Il conteggio alla rovescia dal numero inserito sarà eseguito automaticamente. Specificare un numero compreso fra 1 e 9999.
   - **Utente non può cambiare paaword:** l'utente non è autorizzato a modificare la password.
   - **Disabilita account se utente non login dopo:** l'utente deve modificare la password quando si registra per la prima volta.
   - **Si deve cambiare password in prossimo login xx giorni(s):** se l'utente non si registra nel sistema dopo un certo numero di giorni, l'account si disattiva automaticamente.
   - **Permetti rimozione password di sistema:** questa opzione permette all'utente di rimuovere il database di ID e password dal sistema. Per fare questo, selezionare questa opzione (che può essere abilitata solo dal Supervisore), quindi cercare **PassUnInStall** nella cartella di sistema. Fare clic sul programma e apparirà un messaggio di richiesta di conferma. Fare clic su **Sì** per rimuovere ID e password dal sistema.

Nota: se l'opzione **Permetti rimozione password di sistema** non è selezionata, la perdita delle password richiederà la reinstallazione di Windows e il ripristino delle password stesse.

7.1.2 Modifica di un utente esistente

Solo i supervisori possono modificare le informazioni di un utente di sistema.

1. Selezionare un utente dall'apposito elenco per visualizzarne le proprietà. Oppure fare clic con il tasto destro del mouse sui livelli utente (Utente, PowerUser, Supervisore) e selezionare **Trova account specifico** per la ricerca rapida. Per eseguire le modifiche come supervisore è necessaria una password valida.
2. Modificare le proprietà come necessario. Selezionare l'opzione **L'account è disabilitato**, se si desidera disabilitare questo utente.

7.1.3 Modifica della password al momento del login

1. Quando ci si registra nel sistema, fare clic sul tasto **Change Password (Cambia Password)** nella finestra di dialogo Login. Appare la finestra di dialogo Cambia password.

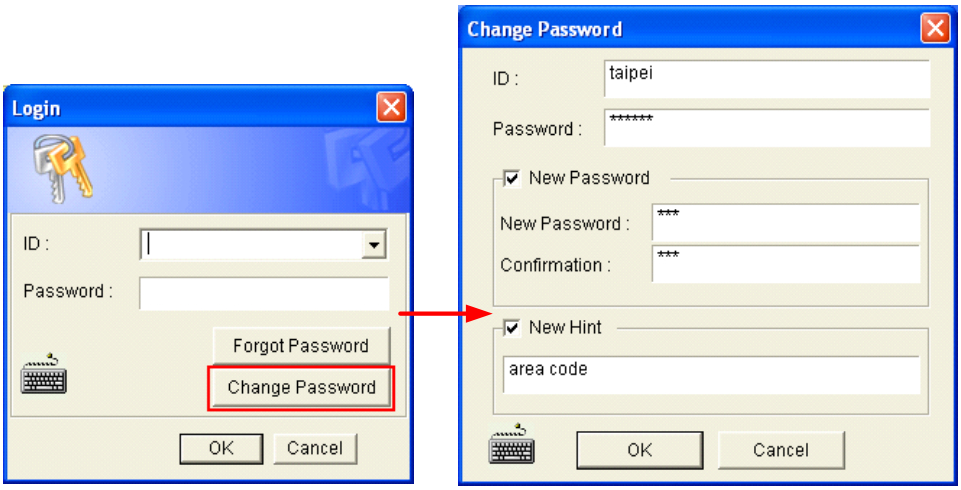


Figura 7-3

2. Digitare le informazioni sulla nuova password e fare clic su **OK** per salvare le modifiche.

Nota: se l'utente non ha il diritto di modificare la password, apparirà il messaggio *Modifica Password/Suggerimento errato*.

7.2 Impostazione notifica

Se si verifica una condizione di allarme, il sistema può attivare automaticamente l'allarme del computer, oltre ad inviare avvisi via SMS ed e-mail ad uno o più destinatari.

7.2.1 Impostazione del server SMS

Prima di poter inviare avvisi via SMS, è necessario configurare il server SMS.

1. Sulla barra dei menu, fare clic su **Strumenti** e selezionare **Impostazioni server SMS**. Appare questa finestra di dialogo.

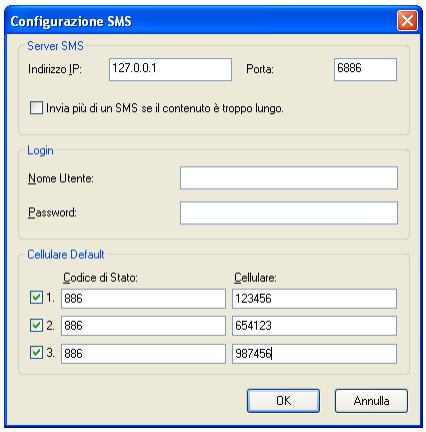


Figura 7-4

2. Digitare l'indirizzo IP del server SMS, nome utente e password di login. Quindi assegnare fino a tre numeri di telefoni cellulari, incluso il prefisso internazionale, a cui inviare l'SMS. Fare clic su **OK**.
3. Per abilitare la connessione SMS, fare clic su Strumenti sulla barra dei menu e selezionare **Connetti a server SMS**.

Nota: Per la codifica ASCII (inglese) i messaggi di testo SMS sono limitati a 160 caratteri, per la codifica Unicode (altre lingue), i messaggi di testo SMS sono limitati a 70 caratteri. Se si desidera inviare messaggi di testo più lunghi, selezionare **Invia più di un SMS se il contenuto è troppo lungo**. I messaggi lunghi verranno suddivisi per un massimo di 9 segmenti ed escono come messaggi SMS multipli.

7.2.2 Impostazione del server e-mail

Prima di poter inviare avvisi via e-mail, è necessario configurare il server e-mail.

1. Sulla barra dei menu, fare clic su **Strumenti** e selezionare **Impostazioni server e-mail**. Appare questa finestra di dialogo.

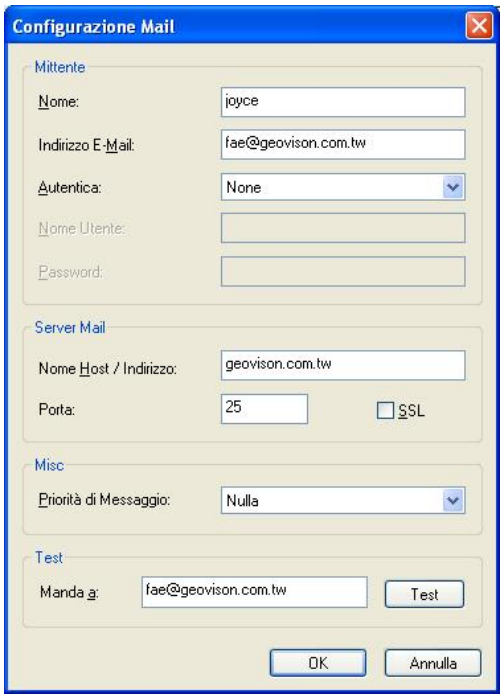


Figura 7-5

2. Impostare le seguenti opzioni:
   - **Nome:** digitare il nome del mittente.
   - **Indirizzo E-Mail:** digitare l'indirizzo e-mail del mittente.
   - **Autentic:** se il server e-mail richiede l'autenticazione per inviare e-mail, selezionare un tipo di autenticazione e digitare una password e un nome utente validi.
   - **Host Nome/Indirizzo:** digitare il nome del server e-mail.
   - **Porta:** mantenere il valore predefinito 25. Altrimenti modificarlo in modo che corrisponda a quello del server e-mail.
   - **SSL:** Abilitare il protocollo Secure Sockets Layer (SSL) per garantire la sicurezza e la privacy della connessione Internet. Quando è abilitata questa opzione, il numero della porta diventa 465.
   - **Priorità di Messaggio:** assegnare una priorità al messaggio, in modo che il destinatario sappia se controllarlo immediatamente (priorità alta) o quando il tempo glielo permette (priorità bassa). Un messaggio ad alta priorità ha un punto esclamativo accanto ad esso. La priorità bassa è indicata da una freccia verso il basso.

- **Manda a:** digitare un indirizzo e-mail valido e fare clic sul tasto Test per controllare che l'impostazione del server sia configurata correttamente.

7.2.3 Impostazione della notifica

1. Sulla barra dei menu, fare clic su **Strumenti** e selezionare **Notifiche**. Appare questa finestra di dialogo.

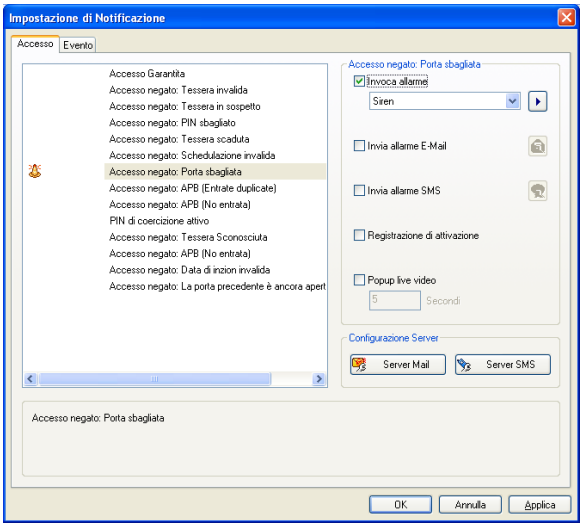


Figura 7-6

2. Utilizzare le schede **Accesso** ed **Evento** per selezionare un evento desiderato per la configurazione dell'avviso.
3. Definire i seguenti tipi di avviso:

- **Invoca allarme:** per abilitare l'allarme del computer se si verifica l'evento selezionato.
- **Invia allarme E-mail:** selezionando questa opzione, appare un'e-mail. Inserire l'indirizzo del destinatario e l'oggetto dell'avviso. Quindi è possibile utilizzare il proprio contenuto o utilizzare i pulsanti sulla finestra del testo per inviare le informazioni programmate automaticamente.
- Ad esempio, facendo clic sul pulsante , l'allarme SMS inviato includerà le informazioni sul controllore. Per i dettagli vedere *Simboli avvisi e-mail e SMS* nell'Appendice.
- **Invia allarme SMS:** selezionando questa opzione, appare una finestra di dialogo. Verificare i numeri di cellulare preimpostati. Selezionare il **tipo di codice del testo**. Quindi digitare i messaggi, altrimenti fare clic sui pulsanti che si trovano sulla finestra del testo per inviare le informazioni programmate automaticamente. Vedere l'esempio in alto in "Invia avviso e-mail".
- **Registrazione di attivazione :** Abilita la registrazione del DVR, Video Server o Compact DVR quando avviene l'evento selezionato. Il tempo di registrazione è tra i 3 e i 6 secondi.

- **Popup live video (Visualizzazione Vista Live):** Verrà visualizzata una vista live associata per gli allarmi quando si verifica l'evento selezionato. È anche possibile specificare la durata della vista live rimanente sullo schermo per un massimo di 300 secondi.

4. Per definire più di un evento con la stessa configurazione degli allarmi, per prima cosa fare clic con il tasto destro del mouse sull'evento precedentemente definito sulla lista e selezionare **Copia** per salvare le sue impostazioni. Quindi usare Ctrl + clic con tasto sinistro o Shift + clic con il tasto desto per selezionare più eventi. Fare clic con il tasto destro sugli eventi selezionati e selezionare **Incolla** per ottenere le stesse impostazioni.

Nota: Per il tipo di codifica selezionare **ASCII** per testi in inglese limitati a 160 caratteri e **Unicode** per testi nelle altre lingue non superiori a 70 caratteri.

7.3 Configurazione di avvio e di backup

È possibile selezionare il server che deve essere abilitato all'avvio di Windows o di ASManager.
È anche possibile specificare un percorso per la funzione di **Backup automatico** per salvare automaticamente un'altra copia dei file di registro e immagine. I file di registro predefiniti e i file immagine sono salvati su :\ASManager\ASRes.

- Per accedere a queste funzioni, fare clic su **Strumenti** sulla barra dei menu e selezionare **Opzione**.

Capitolo 8 ASRemote

Il software client ASRemote è studiato per monitorare più ASmanager nella rete. ASRemote fornisce le seguenti funzioni:

- Monitoraggio remoto
- Visualizzazione live e riproduzione remote
- Controllo remoto: arresto allarmi e blocco/sblocco forzato porte

8.1 Installazione di ASRemote

Inserire il CD contenente il software nel computer e automaticamente apparirà una finestra pop-up. Selezionare **Install GeoVision V1.1 Access Control System (Installa il sistema di controllo dell'accesso GeoVision V1.1)** fare clic su **GeoVision Access Control System (Sistema di controllo accessi GeoVision)** e seguire le istruzioni a video per completare l'installazione.

8.2 La finestra di ASRemote

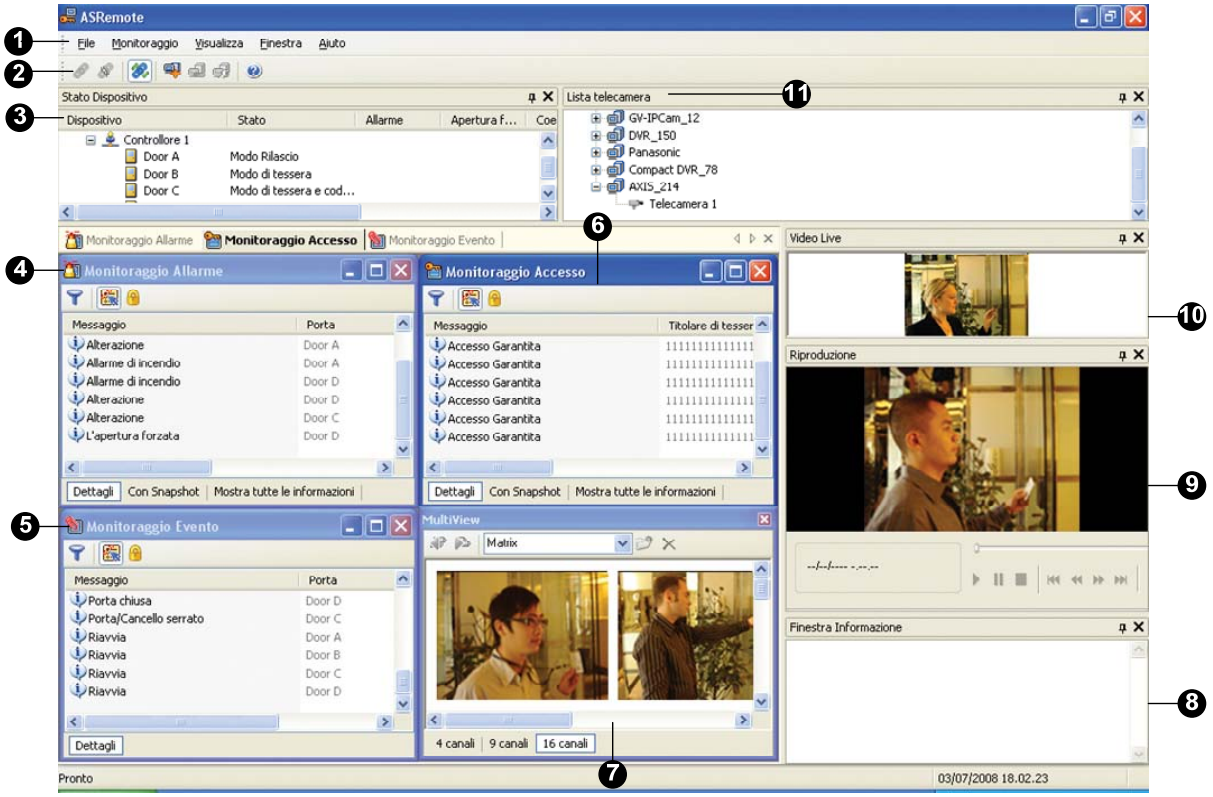


Figura 8-1

N.	Nome	Funzione
1	Barra dei menu	La barra dei menu include le opzioni **File** (accesso/uscita da ASManager), **Monitoraggio** (visualizzazione delle finestre di allarme, accesso ed evento), **Visualizza** (visualizzazione delle finestre delle funzioni) e **Finestra** (organizza la visualizzazione di diverse finestre).
2	Barra degli strumenti	La barra degli strumenti include le opzioni **Connetti, Disconnetti, Connessione automatica, Aggiungi host, Rimuovi host, Impostazioni** e **About (Informazioni)**.
3	Stato dispositivo	Visualizza un elenco di porte connesse e il loro stato corrente.
4	Monitoraggio allarme	Visualizza gli eventi di allarme delle porte.
5	Monitoraggio evento	Visualizza gli eventi monitorati delle porte.
6	Monitoraggio accesso	Visualizza le attività di accesso delle porte.

7	MultiView	Visualizza le viste live delle telecamere connesse da diversi dispositivi IP. Per i dettagli vedere "La finestra MultiView" nel Capitolo 5.
8	Finestra di informazione	Visualizza le informazioni sulle porte, sui lettori e sugli eventi monitorati.
9	Riproduzione	Riproduce gli eventi registrati da un dispositivo IP GeoVision compatibile. Per i dettagli, vedere alcune operazioni in "Recupero del video registrato" del Capitolo 5.
10	Video live	Visualizza la vista live di una delle telecamere connesse. Per i dettagli, vedere alcune operazioni in "Accesso alla vista live" del Capitolo 5.
11	Elenco telecamere	Visualizza un elenco di telecamere connesse.

8.2.1 Barra degli strumenti

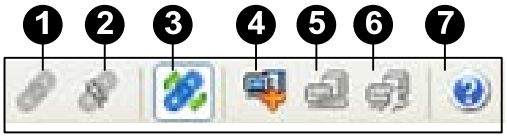


Figura 8-2

Tasti sulla barra degli strumenti di ASRemote:

N.	Nome	Funzione
1	Connetti	Avvia la connessione con ASManager.
2	Disconnetti	Termina la connessione con ASManager.
3	Connessione automatica	Ritenta la connessione con ASManager.
4	Aggiungi host	Aggiunge un host ASManager all'elenco.
5	Rimuovi host	Elimina un host ASManager dall'elenco.
6	Impostazioni	Modifica le impostazioni degli host ASManager.
7	About (Informazioni)	Visualizza la versione di ASRemote.

8.3 Connessione a ASManager

Prima di poter collegare ASRemote ad un ASManager, quest'ultimo deve permettere l'accesso remoto mediante questa procedura:

- Fare clic su **Strumenti** sulla barra dei menu, selezionare **Server** e abilitare **Server di monitoraggio remoto**. Una volta avviato il server, in fondo alla schermata principale appare l'icona .

Per creare un host ASManager e abilitare la connessione ad ASManager:

1. Fare clic sul tasto **Aggiungi Host** sulla barra degli strumenti. Appare questa finestra di dialogo.

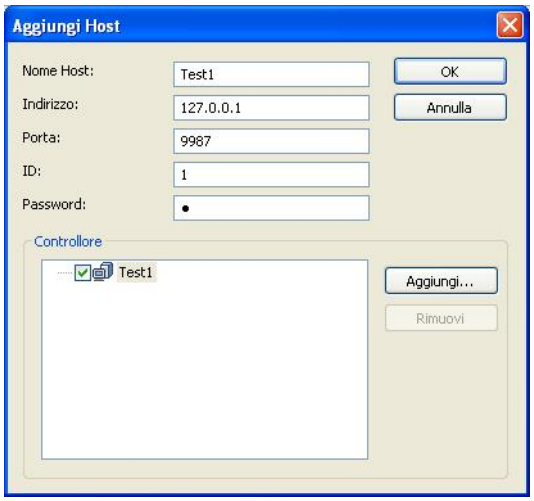


Figura 8-3

2. Assegnare un nome host, digitare l'indirizzo IP di ASManager, modificare il numero della porta (se necessario) e digitare ID e password di login di ASManager.
3. Fare clic su **Aggiungi**. Appare questa finestra di dialogo.

Figura 8-4

4. Digitare l'ID del controller associato ad ASManager e fare clic su **OK**.
5. Per aggiungere più controllori ripetere le istruzioni 3-4.
6. Fare clic su **OK** e tornare alla schermata principale. Nella finestra Stato dispositivo apparirà una cartella host, come illustrato nell'esempio in basso.

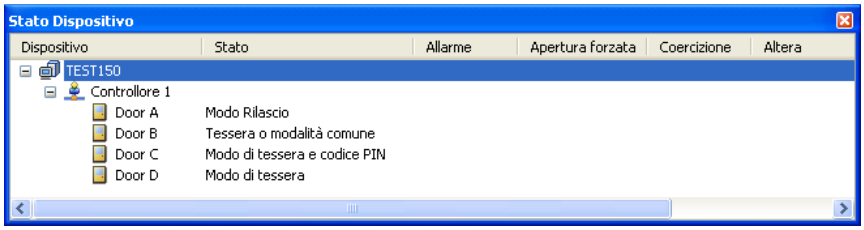


Figura 8-5

Se appare l'icona , significa che è stata stabilita la connessione fra ASManager e ASRemote.

Se appare l'icona , significa che la connessione non è riuscita. Accertarsi che ASManager sia abilitato per la funzione Server di monitoraggio remoto.

Capitolo 9 ASWeb

ASWeb è studiato per eseguire l'interrogazione dei dati degli eventi da ASManager nella rete. Grazie alla connessione ad un ASManager alla volta, gli utenti non solo possono visualizzare i dati degli eventi, ma possono anche scaricare i log in diversi formati.

9.1 Connessione a ASManager

Prima di poter collegare ASWeb ad un ASManager, quest'ultimo deve permettere l'accesso remoto mediante questa procedura:

- Sulla barra dei menu, fare clic su **Strumenti**, selezionare **Server** e abilitare **Server Web**. Appare questa finestra di dialogo.

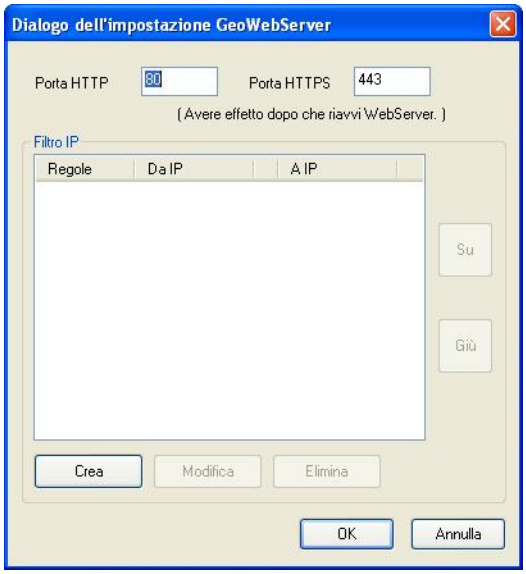


Figura 9-1

Se si desidera garantire o negare l'accesso da alcuni indirizzi IP, fare clic su **Crea** e digitare tali indirizzi. Altrimenti fare clic su **OK** per avviare la connessione. Una volta avviato il server, in fondo alla schermata principale appare l'icona .

Per avviare ASWeb:

1. Aprire il browser Internet e digitare l'indirizzo IP dell'ASManager da collegare.

   Appare questa pagina web.

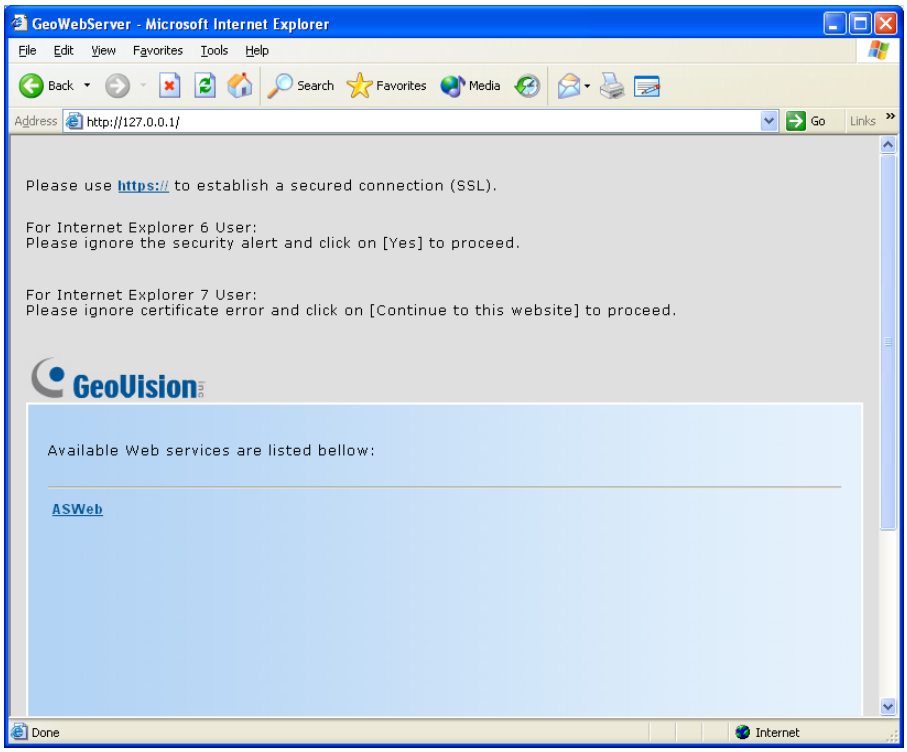

GeoWebServer - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://127.0.0.1/
Go Links
Please use https:// to establish a secured connection (SSL).
For Internet Explorer 6 User:
Please ignore the security alert and click on [Yes] to proceed.
For Internet Explorer 7 User:
Please ignore certificate error and click on [Continue to this website] to proceed.
GeoVision
Available Web services are listed bellow:
ASWeb
Done
Internet

Figura 9-2

2. Fare clic su **https://** per la connessione criptata **SSL** o su **ASWeb** per la connessione normale. Appare una finestra di login.

Figura 9-3

3. Digitare nome utente e password dell'ASManager a cui collegarsi. Appare la pagina ASWeb.

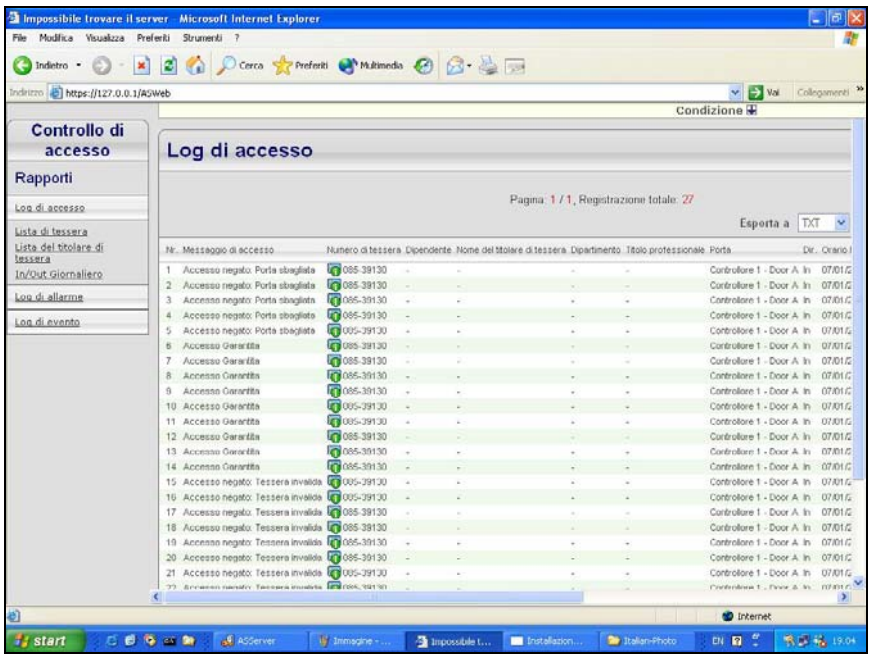


Figura 9-4

9.2 Accedere ai log

È possibile accedere ai log dall'ASManager connesso: Log di accesso, Lista di tessera, Lista del titolare di tessera, In/out giornaliero, Log di allarme e Log di evento. Inoltre, è possibile impostare i criteri di ricerca per visualizzare più efficacemente i registri.

9.2.1 Impostazione dei criteri di ricerca

1. Selezionare il registro che si desidera visualizzare dal riquadro a sinistra. Qui come esempi utilizziamo il Log di accesso.
2. Nella parte superiore della finestra di registro fare clic sul tasto **Freccia in basso** Condition. Appare una finestra di filtro.

3. Digitare o selezionare i criteri di filtrazione desiderati. Ad esempio, vogliamo cercare il log delle registrazioni che soddisfano le condizioni di “Accesso Garantito”, numero di tessera “100012”, entrata anteriore (Dir. di ingr.) e le date dal 20 al 26 agosto. La finestra filtro risultante dovrebbe avere un aspetto simile al seguente:

Figura 9-5

4. Sia nell’elenco a discesa Metti in ordine secondo la condizione primaria, che in quello Metti in ordine secondo la condizione secondaria, selezionare il modo in cui i risultati vengono raggruppati e visualizzati sullo schermo.
5. Nell’elenco a discesa, selezionare **Elenco** per visualizzare un elenco di risultati di ricerca, **Elenco con immagine** per visualizzare un elenco di risultati di ricerca con immagini video associate o **Verifica immagine** per visualizzare le immagini video trovate insieme alle foto del titolare della tessera per poter verificare che l'utente e il titolare siano identici. La dimensione dell’immagine visualizzata e della foto sono anch'esse selezionabili.
6. Fare clic sul tasto **Submit** per avviare la ricerca del log.

9.2.2 Icone della finestra di log

Le icone nella finestra di log possono visualizzare le informazioni della categoria corrispondente. Fare clic sull’icona per visualizzare i dettagli.

: visualizza le informazioni contenute nella tessera.

: indica la disponibilità del video registrato.

: indica la disponibilità dell’immagine video.

Nota: È possible riprodurre il video solo quando il servizio remoto ViewLog incluso nel Control Center Server è abilitato nel DVR. E la funzione Viewlog remoto viene abilitate sul Video Server o sul Compact DVR.

9.2.3 Esportare i log

È possibile scaricare i log dall'ASManager connesso sul computer corrente in tre formati: **.txt**, .**htm** e **.xls**.

1. Utilizzare l'elenco a discesa di Esporta a e selezionare il formato file **TXT**, **HTML** o **Excel**.
2. Utilizzare l'elenco a discesa successivo per selezionare **Questa pagina** e salvare la pagina corrente di log, oppure **Tutto** per salvare tutti i log.
3. Fare clic su **Esporta** per scaricare i log.

9.2.4 Definizione delle colonne

È possibile definire le colonne visualizzate per ciascun tipo di log.

1. Sulla barra dei menu di ASManager, fare clic su **Strumenti** e selezionare il **campo ASWeb**. Appare questa finestra di dialogo.

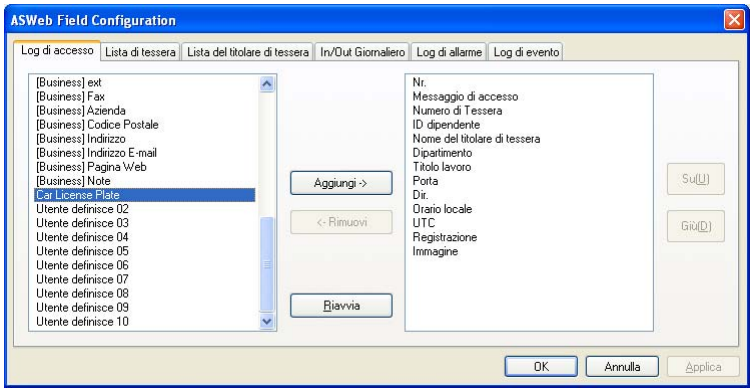


Figura 9-6

2. Fare clic sul pulsante di log desiderato, es. Log di accesso. Le colonne predefinite sono visualizzate sul pannello di destra. Quindi usare **Aggiungi** o **Rimuovi** per definire le proprie colonne di log.

   Ad esempio, abbiamo aggiunto un campo definito dall'utente "Car License Plate (Targa automobilistica)" al Log di accesso. La finestra risultante su ASWeb dovrebbe avere un aspetto simile al seguente:

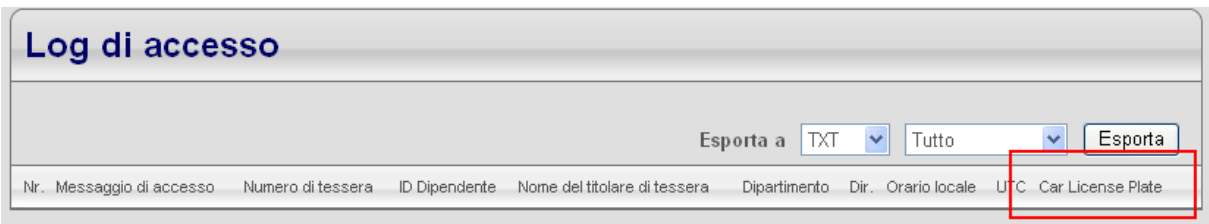


Figura 9-7

Capitolo 10 Risoluzione dei problemi

D1: ASManager non riesce a collegarsi al controllore AS200 via Internet.

Le cause di questo problema possono essere varie, fra cui un conflitto di indirizzo IP, impostazioni di connessione non corrette e problemi di rete. La soluzione è assegnare l'IP fisso rispettivamente ad ASManager e al controllore AS200. In questo modo è possibile determinare se il problema è causato da dispositivi mal funzionanti e da impostazioni di rete non corrette.

1. Disconnettere dalla rete l'hub o lo switch che collega ASManager e il controllore AS200.
2. Assegnare ad ASManager un indirizzo IP fisso NON utilizzato da un altro dispositivo, ad es. 192.168.0.154.

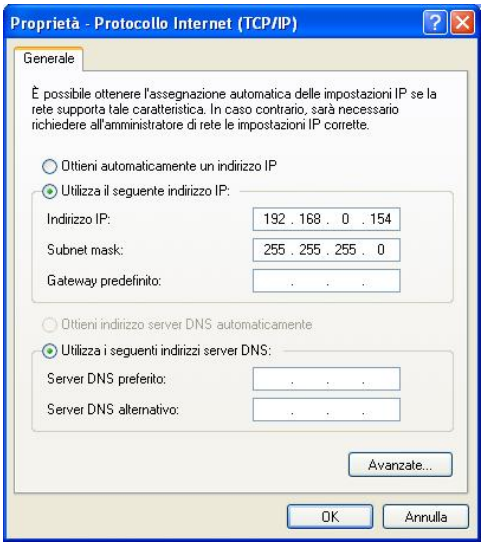

Proprietà - Protocollo Internet (TCP/IP)
Generale
È possibile ottenere l'assegnazione automatica delle impostazioni IP se la rete supporta tale caratteristica. In caso contrario, sarà necessario richiedere all'amministratore di rete le impostazioni IP corrette.
Ottieni automaticamente un indirizzo IP
Utilizza il seguente indirizzo IP:
Indirizzo IP:
192 . 168 . 0 . 154
Subnet mask:
255 . 255 . 255 . 0
Gateway predefinito:
Ottieni indirizzo server DNS automaticamente
Utilizza i seguenti indirizzi server DNS:
Server DNS preferito:
Server DNS alternativo:
Avanzate...
OK
Annulla

Figura 10-1

3. Ripristinare il modulo del controllore AS200 e il modulo Ethernet ai valori predefiniti in fabbrica.
   a. Inserire ASKeypad nel controllore AS 200.
   b. Rimuovere il tappo dal jumper **Predefinito** a due pin.
   c. Premere il pulsante **Reset**.
   d. Rimettere a posto il tappo sul jumper **Predefinito** a due pin.
   e. Per ripristinare il modulo Ethernet, tenere premuto il tasto **EN predefinito** per 6 secondi.
4. Aprire il browser e inserire l'indirizzo predefinito del controllore AS200: http://192.168.0.100

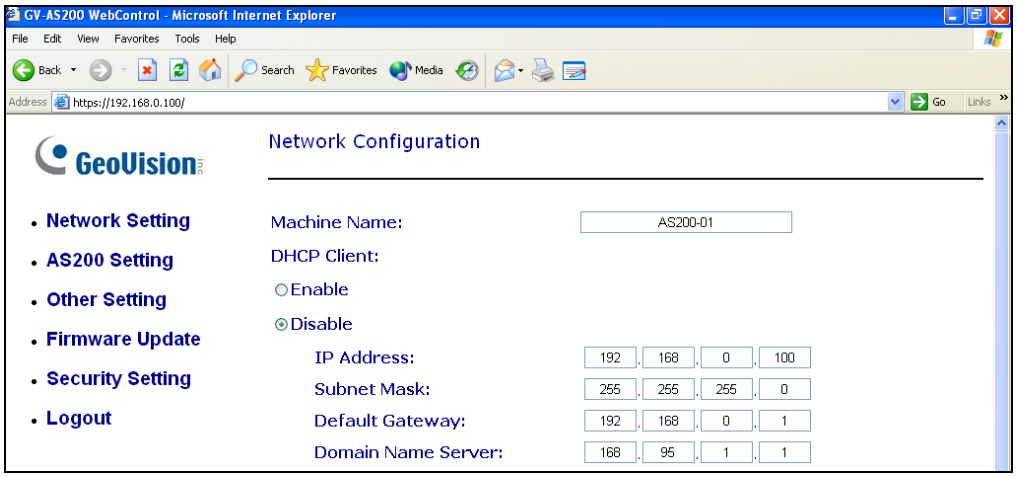


Figura 10-2

5. Nel campo dell'indirizzo IP inserire un indirizzo NON utilizzato da un altro dispositivo, ad es. 192.168.0.XXX.
6. In ASManager inserire le seguenti impostazioni:

   ID Controllore: 1

   Rete: TCP/IP

   IP: 192.168.0.XXX

   Porta: 4000

   Utente: admin

   Password: 1234

   Chiave crypto: 12345678

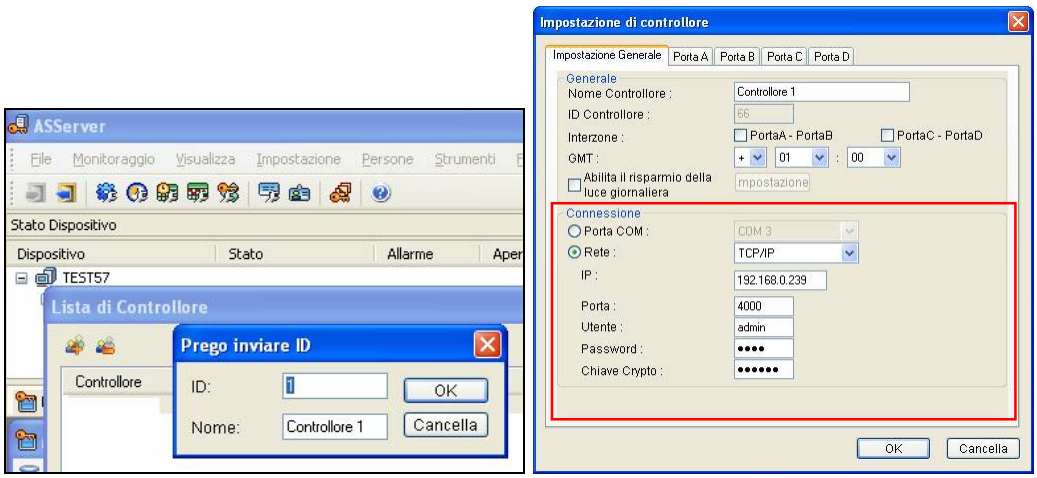


Figura 10-3

7. La connessione fra ASManager e controllore AS200 deve essere stata stabilita e deve apparire l'icona di collegamento . Se la connessione dell'hub o dello switch alla rete cade, potrebbe trattarsi di problemi alla rete stessa. Contattare il proprio amministratore di rete.

D2: La connessione stabilita fra ASManager e il controllore AS200 si è interrotta.

Ciò potrebbe dipendere da un conflitto di indirizzo IP. Seguire queste istruzioni per risolvere il problema:

1. Disconnettere dalla rete l'hub o lo switch che si collega a ASManager e il controllore AS200.
2. Eseguire il **Prompt dei comandi** di Windows. Prendere ad esempio il classico menu start di Windows, fare clic su **Start**, selezionare **Accessori** e fare clic su **Prompt dei comandi**.
3. Digitare **arp-d** e premere **Invio**.

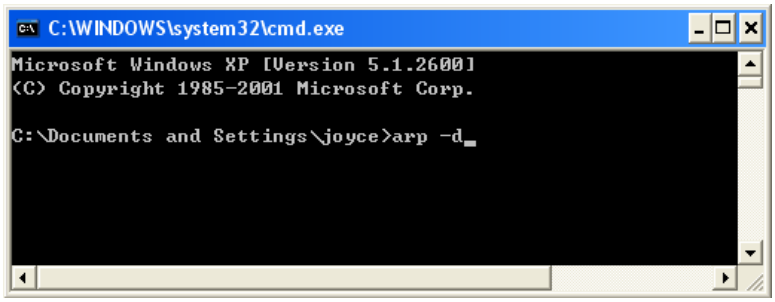


Figura 10-4

4. Assegnare ad ASManager un indirizzo IP fisso NON utilizzato da un altro dispositivo. Vedere figura 10-1.
5. Aprire il browser e inserire l'indirizzo IP assegnato del controllore AS200. Viene visualizzata la pagina con la configurazione di rete. Vedere figura 10-2.
6. Nel campo dell'indirizzo IP inserire un indirizzo NON utilizzato da un altro dispositivo, ad es. 192.168.0.XXX.
7. In ASManager inserire le seguenti impostazioni. Vedere figura 10-3.

   ID Controllore: 1

   Rete: TCP/IP

   IP: 192.168.0.XXX

   Porta: 4000

   Utente: admin

Password: 1234

Chiave crypto: 12345678

8. La connessione fra ASManager e controllore AS200 deve essere stata stabilita e deve apparire l'icona di collegamento . Se la connessione dell'hub o dello switch alla rete cade, potrebbe trattarsi di problemi alla rete stessa. Contattare il proprio amministratore di rete.

D3: ASManager non riceve i messaggi delle tessere, ma il lettore le accetta, quando la connessione fra ASManager e il controllore AS200 è ben stabilita.

Potrebbe dipendere da un problema di memoria del controllore AS200. Ripristinare il modulo del controllore AS200 e il modulo Ethernet ai valori predefiniti in fabbrica. Fare riferimento al punto 3 della domanda 1.

D4: ASManager non riesce a recuperare il video dal DVR per la riproduzione.

1. Accertarsi che il **Servizio remoto Viewlog** su **Control Center Server** sia abilitato sul DVR.
2. Accertarsi che l'ora su ASManager e sul DVR sia la stessa.
3. Accertarsi che il file dell'evento da riprodurre sia stato creato completamente sul DVR. Ad esempio, la durata assegnata di ogni evento registrato sul DVR è 5 minuti. L'evento desiderato di 5 minuti deve essere visualizzato sulla lista eventi ViewLog, in modo da poter accedere al file per riprodurlo.

D5: Dopo aver aggiunto una scheda presentandola al lettore, viene comunque visualizzato il messaggio "*Accesso negato, scheda non valida*".

(Per i dettagli su come aggiungere automaticamente una tessera, vedere Fase 1, 4.3.1 *Aggiungere una singola scheda*).

Potrebbe dipendere dal fatto che il formato della scheda non è compatibile con il controllore AS200. Accertarsi che il lettore sia un dispositivo Wiegand da 26~40 bit. In caso contrario, inviateci le informazioni relative al Vostro formato di tessera, in modo da poterlo personalizzare per Voi.

D6: ASManager non riceve i messaggi delle tessere dal GV-Reader collegato al controllore AS200 attraverso l'interfaccia RS-485.

1. Accertarsi che GV-Reader sia cablato correttamente al controllore AS200 e che lo Switch 4 sia su OFF. Vedere "Collegamento al controllore AS200 mediante l'interfaccia RS-485", *Guida all'installazione di GV-Reader*.
2. Accertarsi che sul controllore AS200 sia impostato l'ID corretto di GV-Reader.
   a. Inserire ASKeypad nel controllore AS 200.
   b. Premere un tasto qualsiasi sulla tastiera, selezionare **Imposta parametro** e premere il tasto ENT YES .
   c. Inserire la password predefinita **1234** e selezionare **Imposta ID GV-Reader** usando i tasti freccia IN ALTO e IN BASSO.
   d. Modificare l'ID GV-Reader 0 in **Wiegand esteso**.

D7: Come lasciare tutte le porte aperte quando viene rilevato un incendio?

Seguire queste istruzioni per cablare il controllore AS200 e impostare ASManager:

1. Collegare insieme i due pin Incendio della Porta A e della Porta B. (indicato come linea rossa)
2. Collegare insieme due pin GND della Porta A e della Porta B. (indicato come linea nera)
3. Collegare il rilevatore di incendi ai pin Incendio e GND della porta A (indicato come linea verde)
4. Collegare il rilevatore di incendi ai pin Incendio e GND della porta B (indicato come linea viola)

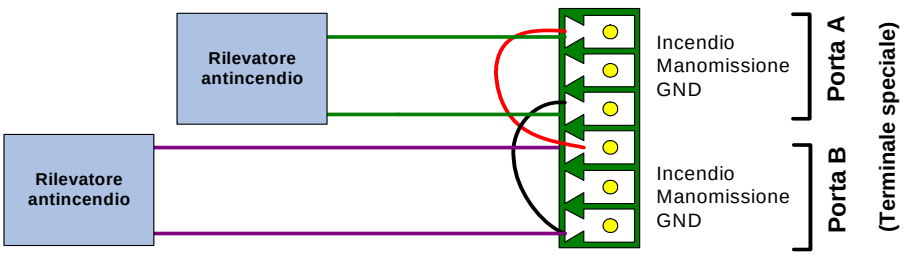


Figura 10-5

5. Nella finestra di dialogo Impostazione di controllore, fare clic sulle schede **Porta A** e **Porta B** e selezionare **Porta Non Serrata** nell'opzione Azione di incendio.

Figura 10-6

D8: Come faccio a ottenere ulteriore supporto?

Visitate il nostro sito web all'indirizzo http:///www.geovision.com.tw

Scriveteci all'indirizzo support@geovision.com.tw

Appendice

A. Dispositivi IP compatibili

N.	Modello	N.	Modello
1	GV-IP Camera	33	JVC VN-C625U
2	GV-Video Server	34	JVC VN-C655U
3	GV-Compact DVR	35	Mobotix M12
4	Arecont AV-1300	36	SONY SNC-CS10
5	Arecont AV-2100	37	SONY SNC-CS11
6	Arecont AV-3100	38	SONY SNC-CS50N
7	Arecont AV-5100	39	SONY SNC-CS50P
8	AXIS 206	40	SONY SNC-DF40N
9	AXIS 207 / AXIS 207W	41	SONY SNC-DF40P
10	AXIS 207MW	42	SONY SNC-DF50N
11	AXIS 210	43	SONY SNC-DF50P
12	AXIS 211	44	SONY SNC-DF70N
13	AXIS 211A	45	SONY SNC-DF70P
14	AXIS 212 PTZ	46	SONY SNC-DF80N
15	AXIS 213 PTZ	47	SONY SNC-DF80P
16	AXIS 214 PTZ	48	SONY SNC-P1
17	AXIS 216FD / AXIS 216FD-V	49	SONY SNC-P5
18	AXIS 221	50	SONY SNC-RX550N
19	AXIS 223M	51	SONY SNC-RX550P
20	AXIS 225FD	52	SONY SNC-RZ25N
21	AXIS 231D+	53	SONY SNC-RZ25P
22	AXIS 232D+	54	SONY SNC-RZ50N
23	AXIS 233D	55	SONY SNC-RZ50P
24	IQEye 301	56	Panasonic BB-HCM110
25	IQEye 302	57	Panasonic BB-HCM311
26	IQEye 510	58	Panasonic BB-HCM331
27	IQEye 511	59	Panasonic BB-HCM371
28	IQEye 701	60	Panasonic BB-HCM381
29	IQEye 702	61	Panasonic BB-HCM403
30	JVC VN-C20U	62	Panasonic BB-HCE481A
31	JVC VN-C205U	63	Panasonic BL-C10
32	JVC VN-C215U	64	Panasonic BL-C30

B. Notifiche degli eventi

- **Eventi “Allarmi”**

Tipo	Descrizione
Apertura forzata	La porta <nome> è stata aperta forzandola.
Anticoercizione	La funzione Anticoercizione è attivata. Vedere “Anticoercizione" in 1.2 *Concetti*
Antimanomissione	Sono stati attivati gli input antimanomissione. Per le impostazioni hardware, vedere *3.2 Connessione degli input* nella guida all’installazione dell’hardware del controllore GV-AS200. Per le impostazioni del software, vedere la Fase 5 nella sezione 4.2.2 della *Fase 2*: *Configurazione di una porta*.
Allarme antincendio	Sono stati attivati gli input antincendio. Per le impostazioni hardware, vedere *3.2 Connessione degli input* nella guida all’installazione dell’hardware del controllore GV-AS200. Per le impostazioni del software, vedere la Fase 5 nella sezione 4.2.2 della *Fase 2*: *Configurazione di una porta*.
Apertura tenuta	La porta <nome> è tenuta aperta per il tempo specificato. Vedere Fase 2 e 5 nella sezione 4.2.2 della *Fase 2: Configurazione di una porta.*
Accesso negato	L’accesso è stato rifiutato.

- **Eventi "Accesso”**

Tipo	Descrizione
Accesso garantito	L’accesso da parte del titolare di tessera <nome> e della tessera <Numero> è avvenuto.
Accesso negato: Tessera non valida	L’accesso è stato rifiutato perché la tessera presentata è sconosciuta.
Accesso negato: Tessera sospesa	L’accesso è stato rifiutato perché la tessera <Numero> è stata sospesa.
Accesso negato: PIN errato	L’accesso è stato negato perché il numero del PIN inserito è errato.
Accesso negato: Tessera scaduta	L’accesso è stato rifiutato perché la tessera <Numero> è scaduta.
Accesso negato: Schedulazione non valida	L’accesso è stato negato perché l’accesso dell’utente non è nella schedulazione programmata.
Accesso negato: Porta errata	L’accesso è stato negato perché l’utente ha acceduto alla porta sbagliata.

Accesso negato: APB (Inserimenti doppi)	L'accesso è stato negato perché è stata violata la funzione Anti-Passback. La tessera <Numero> è stata registrata come inserimento successivo, senza uscita, a un'area sicura. Vedere "Anti-Passback" nella Fase 2, sezione 4.2.2 della *Fase 2: Configurazione di una porta.*
Accesso negato: APB (Nessun inserimento)	L'accesso è stato negato perché è stata violata la funzione Anti-Passback. La tessera <Numero> è stata registrata come uscita, senza inserimento, a un'area sicura.
Accesso negato: APB (Nessuna uscita)	L'accesso è stato negato perché è stata violata la funzione Anti-Passback. La tessera <Numero> è stata registrata come inserimento, senza uscita, a un'area sicura.
Accesso negato: Tessera sconosciuta	L'accesso è stato rifiutato perché il formato della scheda non è compatibile.
Accesso negato: Data di inizio non valida	L'accesso è stato negato perché la tessera <Numero> non è abilitata.
Accesso negato: La porta precedente è ancora aperta (Sincronizzazione)	L'accesso è stato negato perché è stata violata la funzione di sincronizzazione. La porta di ingresso è rimasta aperta. Vedere "Sincronizzazione" nella Fase 5, sezione 4.2.1 della *Fase 1: Configurazione di un controllore per la porta.*

- **Eventi "Evento"**

Tipo	Descrizione
Apertura forzata	La porta <nome> è stata aperta forzandola.
Anticoercizione	La funzione Anticoercizione è attivata. Vedere "Anticoercizione" in 1.2 *Concetti*
Antimanomissione	Sono stati attivati gli input antimanomissione. Per le impostazioni hardware, vedere *3.2 Connessione degli input* nella guida all'installazione dell'hardware del controllore GV-AS200. Per le impostazioni del software, vedere la Fase 5 nella sezione 4.2.2 della *Fase 2*: *Configurazione di una porta*.
Allarme antincendio	Sono stati attivati gli input antincendio. Per le impostazioni hardware, vedere *3.2 Connessione degli input* nella guida all'installazione dell'hardware del controllore GV-AS200. Per le impostazioni del software, vedere la Fase 5 nella sezione 4.2.2 della *Fase 2*: *Configurazione di una porta*.
Apertura tenuta	La porta <nome> è tenuta aperta per il tempo specificato. Vedere Fase 2 e 5 nella sezione 4.2.2 della *Fase 2: Configurazione di una porta.*

Accesso negato	L’accesso è stato rifiutato.
Allarme ripristinato	I suoni degli allarmi sono stati cancellati.
Apertura forzata - ripristinata	L’allarme per apertura forzata è stato cancellato.
Coercizione ripristinata	L’allarme coercizione è stato cancellato.
Antimanomissione ripristinata	L’allarme antimanomissione è stato cancellato.
Allarme antincendio ripristinato	L’allarme antincendio è stato cancellato.
Apertura tenuta ripristinato	L’allarme per apertura tenuta è stato cancellato.
Allarme ripristinato fallito	Impossibile cancellare i suoni degli allarmi.
Cancella evento apertura forzata fallito	Impossibile cancellare allarme per apertura forzata.
Cancella evento coercizione fallito	Impossibile cancellare allarme coercizione.
Cancella evento antimanomissione fallito – Nessun evento presente	Impossibile cancellare allarme antimanomissione.
Cancella evento antimanomissione fallito – Nessun evento presente	Impossibile cancellare allarme antincendio.
Cancella evento apertura tenuta fallito	Impossibile cancellare allarme per apertura tenuta.
Cancella accesso negato fallito	Impossibile cancellare allarme accesso negato.
Cancella evento antimanomissione fallito – I/O ancora non cancellato	Impossibile cancellare allarme antimanomissione poiché gli input antimanomissione rimangono attivi.
Cancella evento antincendio fallito – I/O ancora non cancellato	Impossibile cancellare allarme antincendio poiché gli input antincendio rimangono attivi.
Porta aperta	La porta <nome> è aperta.
Porta chiusa	La porta <nome> è chiusa.
Porta/Barriera non serrata	La porta <nome> non è serrata.
Porta/Barriera serrata	La porta <nome> è serrata.
Regola delle due persone-attiva	La regola delle due persone A/B p attiva quando viene presentata la tessera <numero>.
Regola delle due persone-Conferma	La regola delle due persone A/B è confermata quando la tessera <nome> viene presentata dopo l’altra tessera AB.
Regola delle due persone-Inattiva	La regola delle due persone A/B viene violata quando la tessera <nome> viene presentata successivamente o l’altra tessera AB non viene presentata entro 20 secondi.
Conferma codice tastiera	La password inserita in modo Tessera o Comune è corretta.

Codice tastiera errato	La password inserita in modo Tessera o Comune non è corretta.
Modo rilascio	La porta <nome> è in Modo rilascio. Vedere Fase 4 nella sezione 4.2.2 della *Fase 2: Configurazione di una porta*.
Modo comune o tessera:	La porta <nome> è in Modo comune o tessera. Vedere Fase 4 nella sezione 4.2.2 della *Fase 2: Configurazione di una porta*.
Modo codice PIN e tessera	La porta <nome> è in Modo codice PIN e tessera. Vedere Fase 4 nella sezione 4.2.2 della *Fase 2: Configurazione di una porta*.
Modo tessera	La porta <nome> è in Modo tessera. Vedere Fase 4 nella sezione 4.2.2 della *Fase 2: Configurazione di una porta*.
Modo sblocco antincendio	La porta <nome> è stata sbloccata dopo l'attivazione degli input antincendio. Vedere "Azione antincendio" nella fase 2, sezione 4.2.2 della *Fase 2: Configurazione di una porta*.
Modo blocco antincendio	La porta <nome> è stata bloccata dopo l'attivazione degli input antincendio. Vedere "Azione antincendio" nella fase 2, sezione 4.2.2 della *Fase 2: Configurazione di una porta*.
Sblocco a non serrare in remoto	La porta <nome> non è a serrare in remoto dal server di controllo di ASManager o ASRemote.
Forza a serrare in remoto	La porta <nome> è a serrare in remoto dal server di controllo di ASManager o ASRemote.
Disabilita operazione della porta serrata in remoto	L'evento di "Forza a serrare in remoto" o "Forza a non serrare in remoto" viene cancellato.
Forza a non serrare localmente	La porta <nome> è bloccata sul sito del controllore della porta.
Forza a serrare localmente	La porta <nome> è sbloccata sul sito del controllore della porta.
Disabilita operazione della porta serrata localmente	L'evento di "Forza a serrare localmente " o "Forza a non serrare localmente" viene cancellato.
Ripristina	Controllore porta <nome> è ripristinato.

C. Simboli degli allarmi e-mail e SMS

Icona	Descrizione
	%M (Messaggio): include i messaggi di allarme correlati.
	%T (Controllore): include il nome del controllore della porta.
	%D (Porta): include il nome della porta attivata.
	%L (Ora locale): include l'ora locale.
	%U (UTC): include l'ora UTC.
	%N (Numero di tessera): include il numero di tessera.
	%H (Nome del titolare della tessera): include il nome del titolare della tessera.
	%G (Sesso): include il sesso del titolare della tessera.
	%E (ID dipendente): include l'ID del dipendente.
	%Y (Società): include il nome della società.
	%P (Reparto): include il nome del reparto.
	%F (Ufficio): include il nome dell'ufficio.
	%C (Foto): include la foto del titolare della tessera.
	%S (Immagine): include un'immagine.